目 录

第1章 CLI命令行介绍

本章对 CLI 命令行接口进行详细的描述，主要包括以下内容：

- 访问交换机的CLI
- CLI模式介绍
- 命令语法介绍
- 命令行快捷键
- 历史命令

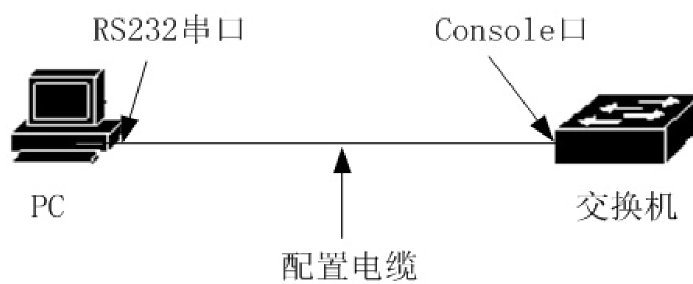
1.1 访问交换机的 CLI

交换机的 CLI 命令行接口提供了用户管理交换机的界面。用户可以通过 Console 口和 Telnet 两种终端来访问交换机的 CLI 命令行接口，下面分别介绍。

1.1.1 用户通过 Console 口访问 CLI

操作步骤如下：

第一步：通过配置电缆把 PC 的串口与交换机的 Console 口连接，如下图：



第二步：启动 PC 机上的终端仿真程序（如 Windows 的超级终端等），配置终端仿真程序的通信参数。终端的通信参数配置如下：

波特率：38400

数据位：8

奇偶校验： 无

停止位：1

数据流控制： 无

超级终端的通信参数配置如下图：



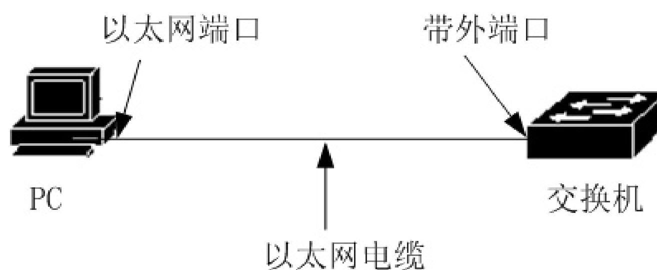
第三步：启动交换机，交换机启动完成后会在终端上显示 CLI 提示符（缺省为 Switch>），用户可以在此提示符下输入命令，这样用户就可以访问交换机的 CLI 了。

1.1.2 用户通过 TELNET 访问 CLI

用户可以通过 iSpirit 8806 交换机的管理模块的带外端口或接口模块的带内端口访问交换机。

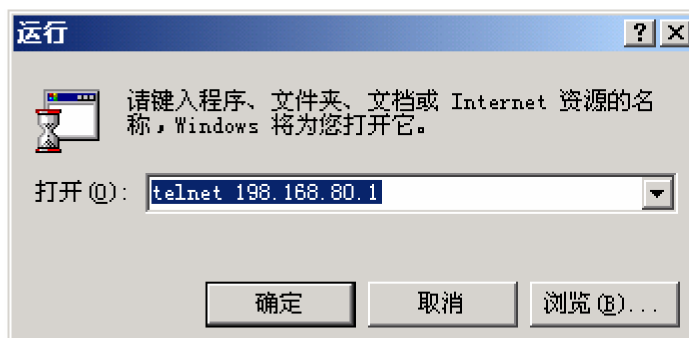
交换机的带外端口的 IP 地址缺省为 198.168.80.1，通过带外端口访问交换机的操作步骤如下：

第一步：通过以太网电缆（必须为交叉线）连接 PC 机的以太网端口和交换机的带外端口。如下图：



第二步：设置 PC 机的以太网端口的 IP 地址，该 IP 地址必须在 198.168.80.0/24 段内（如 IP 地址 198.168.80.100）。通过 ping 198.168.80.1 来判断 PC 机与交换机的连通性。

第三步：如果 PC 机与交换机是连通的，则 Telnet 198.168.80.1 进入 Telnet 终端界面。如下图：



第四步：如果系统没有设置密码，Telnet 界面直接进入 CLI，出现 CLI 提示符（缺省为 Switch>）；如果系统设置了密码，在 Telnet 界面上需要输入密码后才能进入 CLI。

用户通过带内端口访问交换机的方法与通过带外端口访问交换机的类似，但有两点要特别注意：

- 带内端口的 IP 地址是建立在 VLAN 三层接口之上的，在访问交换机之前，必须设置某个 VLAN 接口的 IP 地址，VLAN1 的缺省 IP 地址是 192.168.0.1，可以直接使用。VLAN 接口的 IP 地址可以通过 Console 口或带外端口 Telnet 界面进行配置。
- 用户通过带内端口访问交换机，可以直接通过以太网电缆连接 PC 和带内端口，也可以通过一个网络进行连接，只需要 PC 与交换机的某个 VLAN 之间能够互通就行了。

1.2 CLI 模式介绍

1.2.1 CLI 模式的作用

CLI 模式的作用主要有如下两点：

- 方便对用户的分级，防止未授权的用户非法使用 CLI。

用户可分为两个级别，也就是两类：普通用户和特权用户。

普通用户只能查看交换机的一些运行状态，只能使用显示命令。

特权用户除了能够查看交换机的运行状态以外，还可以对交换机进行维护和配置，改变交换机的行为。

- 方便用户对交换机进行配置

交换机存在很多的配置，如果把所有的配置放在一个模式中，用户使用起来非常不方便。为此，在 CLI 上建立多个模式，把相近的命令放在一个模式中，便于用户的理解和使用。如把与 VLAN 相关的命令放在 VLAN 配置模式中，把与接口相关的命令放在接口配置模式中。

1.2.2 CLI 模式的标识

CLI 提示符是 CLI 模式的标识，用户在使用 CLI 时，通过看 CLI 提示符就知道目前所处的 CLI 模式。

CLI 提示符由两部分组成，一部分标识主机，另一部分标识模式。

CLI 提示符中的主机部分使用的是系统的主机名，系统的主机名是可配置的，缺省为 Switch，所以 CLI 提示符缺省是以 Switch 开头，后面提到的 CLI 描述符一般情况都使用缺省的主机名。

CLI 提示符中的模式部分是不可配置的，每种模式都有自己对应的模式字符串，有些模式字符串是固定不变的，而有些模式字符串是可变的。如 VLAN 配置模式的模式字符串是固定的，接口配置模式的模式字符串是可变的。

例如：

CLI 提示符 Switch#标识特权模式，Switch 标识主机，而#标识模式。

CLI 提示符 Switch(config-ge1/1)#标识接口配置模式，并且配置的是 ge1/1 端口，Switch 标识主机，而(config-ge1/1)#标识模式。

CLI 提示符 Switch(config-vlan2)#标识接口配置模式，并且配置的是 vlan2 接口，Switch 标识主机，而(config-vlan2)#标识模式。

1.2.3 CLI 模式的分类

CLI 模式分为普通模式，特权模式，全局配置模式和配置子模式四大类，而配置子模式由很多个 CLI 模式组成。

普通用户只能访问普通模式，特权用户可以访问所有的 CLI 模式。

Console 和 Telnet 终端首先进入的是普通模式，在普通模式下输入 enable 命令并且成功验证密码后进入特权模式。在 Telnet 终端上，普通用户只能停留在普通模式下，不能进入特权模式。在特权模式下输入 configure terminal，CLI 模式进入全局配置模式。在全局配置模式下输入相关的命令可以进入各配置子模式。

下表列出了交换机的主要的 CLI 模式：

模式	描述	提示符	进入模式的命令	退出模式的命令
普通模式	提供了显示命令查看交换机的状态信息。	Switch>	终端首先进入的模式。	在 Console 终端上没有退出模式的命令，在 Telnet 终端上使用 exit 或 quit 命令退出 Telnet 终端。
特权模式	除了提供显示命令查看交换机的状态信息外，还提供了调试，版本升级和配置维护等命令。	Switch#	在普通模式下输入 enable 命令。	使用 disable 命令退回到普通模式。 在 Console 终端上使用 exit 或 quit 命令退到普通模式，在 Telnet 终端上使用 exit 或 quit 命令退出 Telnet 终端。
全局配置模式	提供了不能在配置子模式内实现的通用命令，如配置静态路由命令。	Switch(config)#	在特权模式下输入 configure terminal 命令。	使用 exit，quit 或 end 命令退出到特权模式。
接口配置模式	提供了配置端口和 VLAN 接口的命令。端口又可分为千兆和万兆端口。	千兆端口： Switch(config-ge2/1)# 万兆端口： Switch(config-xe1/1)# VLAN 接口： Switch(config-vlan1)#	在全局配置模式下输入 interface <if-name> 命令。	使用 exit 或 quit 命令退出到全局配置模式，使用 end 命令退出到特权模式。
VLA	提供了配置 VLAN 的	Switch(confi	在全局配置模	使用 exit 或 quit 命令退出到全

N 配置模式	命令。例如创建和删除 VLAN 的命令。	g-vlan)#	式下输入 vlan database 命令。	局配置模式，使用 end 命令退出到特权模式。
MSTP 配置模式	提供了配置 MSTP 的命令。例如创建和删除 MSTP 实例的命令。	Switch(config-mst)#	在全局配置模式下输入 spanning-tree mst configuration 命令。	使用 exit 或 quit 命令退出到全局配置模式，使用 end 命令退出到特权模式。
RIP 配置模式	提供了配置RIP协议的命令，例如指定启动RIP的IP网段的命令。	Switch(config-rip)#	在全局配置模式下输入 router rip 命令。	使用 exit 或 quit 命令退出到全局配置模式，使用 end 命令退出到特权模式。
OSPF 配置模式	提供了配置 OSPF 协议的命令，例如指定启动 OSPF 的 IP 网段的命令。	OSPF 进程 0 的提示符：Switch(config-ospf)# OSPF 进程 1 的提示符：Switch(config-ospf-1)#	在全局配置模式下输入 router ospf [ospf-id] 命令。	使用 exit 或 quit 命令退出到全局配置模式，使用 end 命令退出到特权模式。
VRRP 配置模式	提供了配置 VRRP 协议的命令，例如指定 VRRP 的虚拟 IP 地址的命令。	Switch(config-vrrp)#	在全局配置模式下输入 router vrrp <if-name> <vrid>命令。	使用 exit 或 quit 命令退出到全局配置模式，使用 end 命令退出到特权模式。
终端配置模式	提供了配置 Console 和 Telnet 终端的命令，如配置终端的超时时间的命令。	Switch(config-line)#	在全局配置模式下输入 line vty 命令。	使用 exit 或 quit 命令退出到全局配置模式，使用 end 命令退出到特权模式。
模块配置	提供了配置接口模块的命令，如创建	Switch(config-module)#	在全局配置模式下输入	使用 exit 或 quit 命令退出到全局配置模式，使用 end 命令退

模式	和删除模块的命令等。		module-management 命令。	出到特权模式。
密钥链配置模式	提供了配置密钥链的命令，如创建和删除密钥链的命令等。	Switch(config-keychain)#	在全局配置模式下输入 key chain <name> 命令。	使用 exit 或 quit 命令退出到全局配置模式，使用 end 命令退出到特权模式。

1.3 命令语法介绍

1.3.1 命令组成

CLI 命令由关键字和参数两部分组成，第一个词必须是关键字，后面的词可以是关键字也可以是参数，关键字和参数可以交替出现。一个命令必须有关键字，但可以没有参数。例如命令 write 就只有一个关键字而没有参数；命令 show version 有两个关键字而没有参数；命令 vlan <vlan-id> 有一个关键字并且有一个参数； 命令 instance <instance-id> vlan <vlan-id>有两个关键字和两个参数并且关键字和参数是交替出现的。

1.3.2 参数类型

CLI 命令的参数分为两种： 必选参数和可选参数。在输入命令时必选参数必须输入，而可选参数可以输入也可以不输入。如命令 vlan <vlan-id>中的参数是必选参数，在输入命令时此参数必须输入；而命令 show interface [if-name]中的参数是可选参数，在输入命令时此参数可输入，也可不输入。

1.3.3 命令语法规则

在用文本描述命令时必须满足以下规则：

1）关键字直接用单词表示。

如命令 show version。

2）参数必须用< >括起来。

如命令 vlan <vlan-id>

3）如果是一个可选参数，参数必须用[ ]括起来。

如命令 show vlan [<vlan-id>]

对于这种情况，参数的< >可以省略，改成：

命令 show vlan [vlan-id]

也就是参数 vlan-id 可以输入，也可以不输入。

如果是一个必选参数，参数不能有[ ]。

4）如果有多个关键字或参数中必须选择一个，用{ }把多个关键字或参数括起来，多个关键字或参数之间用 | 隔开， | 前后都需要一个空格。

如多个关键字必选的命令：

spanning-tree mst link-type {point-to-point | shared}

在 point-to-point 和 shared 之间必须选择一个。

多个参数必选的命令：

no arp {<ip-address> | <ip-prefix>}

关键字和参数混杂必选的命令：

vrrp authentication {none | simple-password <password>}

5）如果多个关键字或参数中可选一个，用[ ]把多个关键字或参数括起来，多个关键字或参数之间用 | 隔开， | 前后都需要一个空格。

命令如下：

debug rip packet [recv | send]

关键字 recv 和 send 可以选择一个，也可以不选。

show ip route [<ip-address> | <ip-prefix>]

show interface [<if-name> | switchport]

6）如果有一个关键字或参数或一组关键字或参数可以重复选择输入，在这个（组）关键字或参数后加符号“*”。

例如 ping 命令：

ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*

-j <count> <ip-address>* --- 可以重复输入多个 IP 地址

-k <count> <ip-address>* --- 可以重复输入多个 IP 地址

整个选项也可以重复输入。

6）参数用一个或多个单词的描述符表示，如果是多个单词，用符号“-”隔开每个单词，每个单词都是小写。

正确的参数表示法：<vlan-id>，<if-name>，<router-id>， <count>等。

错误的参数表示法：<1-255>，<A.B.C.D>，<WORD>，<IFNAME>等。

1.3.4 命令缩写

用户在 CLI 界面上输入命令时，命令的关键字可以缩写。CLI 支持命令的前缀匹配功能，只要输入的词与关键字前缀唯一匹配，CLI 就把输入的词解析成匹配的关键字。这样用户在使用 CLI 时非常方便，用户可以键入很少的字符完成一个命令，例如 show version 命令可以只键入 sh ver。

1.3.5 语法帮助

CLI 命令行接口中设置有语法帮助，支持每一级命令和参数的帮助功能，分别描述如下：

1）在某个 CLI 模式下直接输入？键，在终端上会列出该模式下的所有命令的第一个关键字及其描述。例如 Switch(config)#?。

2）输入一个命令中的前面的部分，然后输入空格后再输入？键，在终端上会列出下一级的所有关键字或参数及其描述。例如 Switch#show ?。

3）输入一个不完整的关键字后直接输入？键，在终端上会列出与此输入前缀匹配的所有关键字及其描述。例如 Switch#show ver?。

4）输入一个命令中的前面的部分，然后输入空格后再输入 Tab 键，在终端上会列出下一级的所有关键字，下一级如果是参数，则不会列出来。

5）输入一个不完整的关键字后直接输入 Tab 键，如果只有一个关键字与此输入前缀匹配，则直接补齐，如果有多个关键字与此输入前缀匹配，则在终端上列出所有匹配的关键字。

1.3.6 命令行错误信息

用户输入的命令如果没有通过语法检查，会在终端上显示错误信息，常见的错误信息如下表。

错误信息	错误原因
Invalid input 或 Unrecognized command	没有找到匹配的关键字。 参数输入不对。 输入的关键字或参数太多。
Incomplete command	命令输入不完整，还有关键字或参数没有输入。
Ambiguous command	关键字输入不完整，有多个关键字与输入前缀匹配。

1.4 命令行快捷键

1.4.1 行编辑快捷键

CLI 命令行接口支持行编辑快捷键功能，行编辑快捷键可以方便 CLI 命令的输入和编辑。用户在输入或编辑命令时，可以使用行编辑快捷键加速命令的输入。下表列出所有的行编辑快捷键及实现的功能：

快捷键	功能
Ctrl+p 或↑键	上一条命令
Ctrl+n 或↓键	下一条命令
Ctrl+u	删除整行
Ctrl+a	光标回到行首
Ctrl+f 或→键	光标向右移动一格
Ctrl+b 或←键	光标向左移动一格
Ctrl+d	删除光标所在的字符
Ctrl+h	删除光标前一个字符
Ctrl+k	删除光标处及光标后的所有字符
Ctrl+w	删除光标前的所有字符

Ctrl+e	光标移到行尾
Ctrl+c	中断，不执行命令行。如果 CLI 处在全局配置模式或者是配置子模式，CLI 退到特权模式；如果 CLI 处在普通模式或特权模式，CLI 模式保持不变，但 CLI 另起新行。
Ctrl+z	与 Ctrl+c 功能相同。
Tab	输入不完整的关键字后使用此键，如果有一个关键字与输入的前缀匹配，则补齐此关键字；如果有多个关键字与输入的前缀匹配，则列出所有匹配的关键字；如果没有关键字匹配，则此键无效。

注意：有些 Console 终端上↑、↓、→、←键不可用。

1.4.2 显示命令快捷键

对于以 show 关键字开头的命令都是显示命令，有些显示命令由于显示的内容很多，在一屏中无法显示完，终端提供了分屏显示的功能。在显示一屏后终端等待用户输入来决定后面的处理。下表列出了显示命令快捷键及其功能。

快捷键	功能
空格 Space	显示下一屏
回车 Enter	显示下一行
Ctrl+c	中断命令的执行，退出到 CLI 模式下。
其它键	与 Ctrl+c 功能相同。

1.5 历史命令

CLI 命令行接口支持命令的历史记录功能，能记住用户最近使用的 20 个历史命令，把用户最近键入的命令保存起来。您可以用 show history 来显示已经输入过的命令，您也可以用 Ctrl+p,Ctrl+n 或↑、↓键来选择历史命令。历史命令功能可以方便用户输入命令。

第2章 系统管理配置

用户在学习交换机的相关功能配置之前，需要先掌握交换机的系统管理和维护方面的一些基本配置，本章就描述这些系统管理和维护的基本配置，主要包括以下内容：

- 系统安全配置
- 系统维护和调试
- 系统监控
- 配置文件管理
- 软件版本升级

2.1 系统安全配置

为了防止非法用户入侵交换机，系统提供了几种系统管理安全方面的措施，主要包括：

- 多用户管理控制
- Telnet密码控制
- enable密码控制
- Telnet服务控制
- 源IP地址控制

2.1.1 多用户管理控制

多用户管理既保证了交换机系统的安全，又提供了多个用户同时对交换机进行管理和维护的能力。多用户管理通过给每个用户一个用户名、密码和权限来保证系统安全的，用户在访问交换机时首先需要验证用户名和密码，只有用户名和密码都正确并且一致时才能验证通过。用户通过验证后能够访问交换机，但用户的权限限定了用户访问交换机的范围。

多用户管理把用户的权限分为两级：普通用户和特权用户。普通用户只能停留在CLI命令行接口的普通模式，只能够使用显示命令，查询交换机的信息。特权用户可以访问CLI命令行接口的所有模式，可以使用CLI提供的所有命令，既可以查询交换机的信息，又可以对交换机进行维护和管理。

多用户管理功能只应用于Telnet终端，不控制Console终端。在使用Console终端访问交换机时不需要验证用户名和密码，用户可以直接访问CLI。而通过Telnet终端访问交换机时需要验证用户名和密码，只有用户名和密码都验证通过后才能够访问CLI。

交换机缺省没有用户，也就是说缺省没有启用多用户管理功能，此时登陆Telnet终端不需要进行用户名和密码验证。当使用命令增加一个用户名时，多用户管理功能就被启用了，此时Telnet终端需要进行用户名和密码验证。当使用命令删除了所有的用户时，多用户管理功能又被关闭了，系统回到了缺省状态。

多用户管理相关的命令如下表：

命令	描述	CLI模式
username <user-name> password <key> {normal |	增加一个用户，如果指定的用户已经存在，则修改该用	全局配置模式

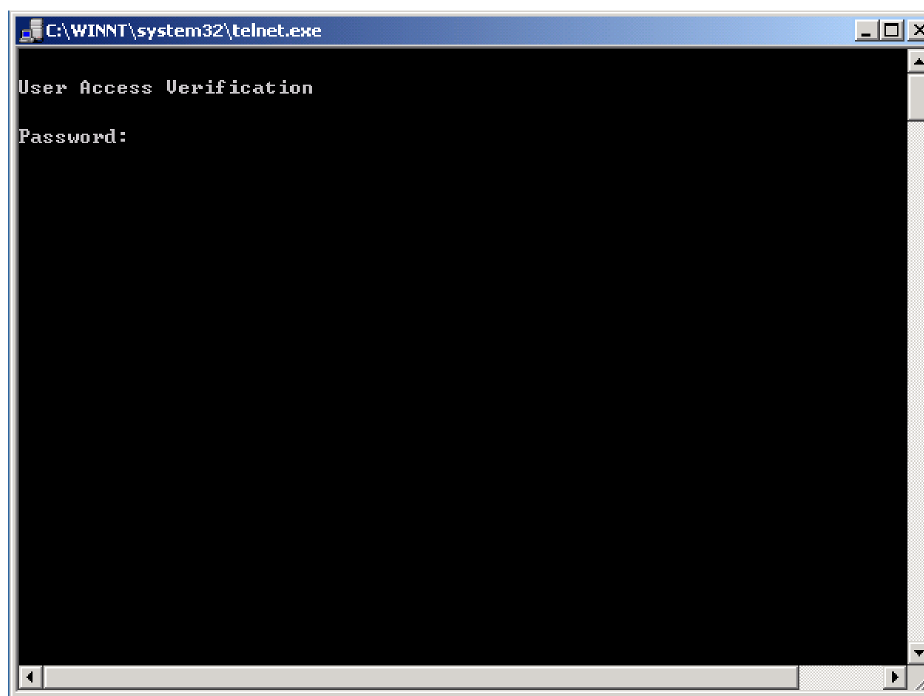
privilege}	户的密码和权限。第一个参数是用户名，第二个参数是密码，可选项表示权限，normal 表 示 普 通 用 户 ，privilege表示特权用户。	
no username [user-name]	删除一个或全部的用户。如果不输入参数，表示删除所有的用户，如果输入参数，表示删除一个指定的用户名的用户。	全局配置模式
show running-config	查看系统当前配置，可以查看到多用户管理的配置。	特权模式

2.1.2 Telnet 密码控制

当多用户管理没有启用时，用户登陆Telnet终端不需要进行用户名和密码检查，可直接访问Telnet的CLI。为提高系统的安全性，交换机增加了Telnet密码来对Telnet访问进行控制。当交换机设置了Telnet密码并且多用户管理没有启用时，用户登陆Telnet终端时需要做Telent密码检查，只有输入了正确的密码才能够访问CLI。如果系统启用了多用户管理，Telnet密码就不会生效，用户访问Telnet终端不做Telnet密码检查，而是做多用户管理的用户名和密码检查。

交换机缺省没有设置Telnet密码，在这种情况下，用户访问Telnet终端时不需要进行Telnet密码验证。

下图为用户登陆Telnet终端的界面，在此界面下输入Telnet密码。



Telnet密码的相关命令如下表：

命令	描述	CLI模式
password <key>	设置Telnet密码。	全局配置模式
no password	清除Telnet密码。	全局配置模式
show running-config	查看系统当前配置，可以查看到Telnet密码的配置。	特权模式

注意：为了系统的安全，管理员需要设置系统的Telnet密码。

2.1.3 enable 密码控制

enable密码用于控制普通模式到特权模式的切换，在enable密码验证前，用户只能查看交换机的信息，而enable密码验证后，用户就有可能对交换机进行配置和维护。

enable密码不依附于用户，任何用户登陆到Console终端或Telnet终端，如果要进入特权模式都必须验证enable密码，如果验证不成功，则只能停留在普通模式下。

在普通模式下输入enable命令，终端会提示用户输入密码，此时用户可输入enable密码，如果密码验证成功，终端进入特权模式，否则，停留在普通模式，对于普通用户来说不管密

码是否验证成功都不能进入特权模式。

enable密码缺省为空，这种情况下在普通模式下输入enable命令后终端不提示输入密码直接进入特权模式。

enable密码的相关命令如下表：

命令	描述	CLI模式
enable password <key>	设置系统的enable密码。	全局配置模式
no enable password	清除系统的enable密码，enable密码为空。	全局配置模式
show running-config	查看系统当前配置，可以查看到enable密码的配置。	特权模式
enable	交互式命令，验证系统的enable密码，验证成功后，终端进入特权模式。	普通模式

注意：为了系统的安全，管理员需要设置系统的enable密码。

2.1.4 Telnet 服务控制

在有些情况下，管理员不需要远程管理交换机，只需要在本地通过Console终端来管理交换机就行了，此时为了提高系统的安全性，防止非法用户远程登陆Telnet终端，管理员可以关闭Telnet服务。Telnet服务缺省是打开的。

Telnet服务控制的相关命令如下表：

命令	描述	CLI模式
enable telnet [number]	打开Telnet服务。number参数的范围为1到100，缺省为5。	终端配置模式
disable telnet	关闭Telnet服务。	终端配置模式
show running-config	查看系统当前配置，可以查看到Telnet服务控制的配置。	特权模式

2.1.5 源 IP 地址控制

在需要远程管理交换机的情况下，为了提高系统的安全性，可以通过源IP地址控制的方法来实现系统的安全管理。如果允许某个IP地址访问交换机，则使用该IP地址的PC可以登陆Telnet终端，如果禁止某个IP地址访问交换机，则使用该IP地址的PC无法登陆Telnet终端。

源IP地址控制要使用到ACL资源库，在实施之前，需要先配置标准ACL规则组，在规则组中定义一条或多条源IP地址的过滤规则。在配置源IP地址控制时，直接使用ACL组名。

缺省情况下系统没有实施源IP地址控制，任何与交换机能够连通的PC都能登陆到Telnet终端。当然，在Telnet服务是关闭的情况下，源IP地址控制没有任何意义。

源IP地址控制的相关命令如下表：

命令	描述	CLI模式
access-class <acl-name>	指定一个ACL组，打开源IP地址控制，如果指定的ACL组不存在或不是标准ACL组，则不对源IP地址进行控制。	终端配置模式
no access-class	关闭源IP地址控制。	终端配置模式
show running-config	查看系统当前配置，可以查看到源IP地址控制的配置。	特权模式

2.2 系统维护和调试

基本的系统维护和调试功能主要包括以下内容：

- 配置系统的主机名
- 配置系统的时钟
- 配置终端超时属性
- 系统复位
- 查看系统信息

- 网络连通性调试
- Traceroute调试

2.2.1 配置系统的主机名

系统的主机名用于标识交换机，方便用户区分不同的交换机，同时系统的主机名还是终端的CLI提示符的一部分。系统的主机名缺省是Switch。

系统的主机名的相关命令如下表：

命令	描述	CLI模式
hostname <name>	设置系统的主机名。	全局配置模式
no hostname	清除系统的主机名，即主机名回到缺省值Switch。	全局配置模式
show running-config	查看系统当前配置，可以查看到系统的主机名的配置。	特权模式

2.2.2 配置系统的时钟

交换机提供了实时时钟的功能，通过命令可以设置当前时钟，也可以查看当前时钟。系统的时钟由内部供电，保证系统断电时实时时钟的持续运行，系统启动后不需要重新设置时钟。

交换机在出厂时已经设置好时钟，用户不需要再进行设置，如果用户发现时间不准时，用户可以重新设置时钟。

系统时钟的相关命令如下表：

命令	描述	CLI模式
set date-time <year> <month> <day> <hour> <minute> <second>	设置系统的当前时钟，需要输入年、月、日、小时、分和秒参数。	特权模式
show date-time	显示系统的当前时钟。	普通模式，特权模式

2.2.3 配置终端超时属性

为了终端的安全性，当终端没有键输入的情况下，超过一定的时间，终端会做退出处理。Console终端和Telnet终端的退出处理不一样，对于Console终端，当终端超时时，CLI模式退到普通模式，对于Telnet终端，当终端超时时，Telnet连接中断，Telnet终端退出。

终端超时时间缺省为10分钟，用户也可以设置终端永远不超时。

终端超时的相关命令如下表：

命令	描述	CLI模式
exec-timeout <minutes> [seconds]	设置终端超时时间，如果参数都为0时，表示终端永远不超时。	终端配置模式
no exec-timeout	设置终端超时时间回到缺省情况，即10分钟。	终端配置模式
show running-config	查看系统当前配置，可以查看到终端超时的配置。	特权模式

2.2.4 系统复位

系统提供了以下几种复位方法：

- 复位管理模块自身
- 复位某个接口模块
- 复位整个交换机系统

系统复位的相关命令如下表：

命令	描述	CLI模式
reset	复位管理模块自身，不影响接口模块。	特权模式
reset module <module-id>	复位某个接口模块，参数是1到5。	特权模式
reset system	复位整个交换机系统，包括所有在	特权模

	位的管理模块和接口模块。	式

2.2.5 查看系统信息

系统提供了丰富的显示命令来查看系统的运行状态和系统的信息，这里只列出几个常用的系统维护的显示命令，如下表：

命令	描述	CLI模式
show version	显示系统的版本号和执行文件编译连接的时间。	普通模式，特权模式
show bdver	显示所有的管理模块和接口模块的版本号。	普通模式，特权模式
show snmp system information	显示系统的基本信息，包括系统启动后运行了多长时间。	普通模式，特权模式
show history	显示在CLI命令行上最近输入的命令列表。	普通模式，特权模式

2.2.6 网络连通性调试

为了调试交换机与网络中的另一设备的连通性，需要在交换机上实现ping命令，在交换机上ping对方的IP地址，如果交换机收到对方来的ping应答，说明两端是连通的，否则表明两端不能进行通信。

交换机不仅实现了ping命令，还在ping命令上支持很多选项，用户通过使用这些选项进行更加精确和复杂的调试。

ping命令如下表：

命令	描述	CLI模式
ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k	在使用时可以不带任何选项，也可以带一个或多个选项。如果不带任何选项，就	特权模式

<count> <ip-address>* | -w <timeout>]*	是最简单的ping命令。命令在执行时可键入Ctrl+c中断命令的执行。	

2.2.7 Traceroute 调试

为了调试交换机与网络中的另一设备在通信时经过了哪些中间设备时，需要在交换机上实现trace-route命令。在交换机上使用trace-route命令时，指定对方的IP地址，命令执行过程中会把中间经过的路径全部显示出来。

交换机不仅实现了trace-route命令，还在trace-route命令上支持很多选项，用户通过使用这些选项进行更加精确和复杂的调试。

trace-route命令如下表：

命令	描述	CLI模式
trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*	在使用时可以不带任何选项，也可以带一个或多个选项。如果不带任何选项，就是最简单的trace-route命令。命令在执行时可键入Ctrl+c中断命令的执行。	特权模式

2.2.8 Telnet 客户端

iSpirit8806交换机提供Telnet客户端功能，用户可以通过Telnet客户端远程访问其他的设备。

命令	描述	CLI模式
telnet <ip-address>	参数是目标设备的IP地址	特权模式

2.3 系统监控

iSpirit8806交换机提供环境监测的功能，防止由于不合理的电压、温度对机器造成损坏和不能正常工作，为用户提供实时机器运行状况的功能。环境监控负责收集主控板和线板上各测量点的温度和电压，在普通模式或特权模式下通过show temperature和show voltage命令查看系统温度或者电压信息，该命令后跟一个可选参数slot决定要查看的对象是哪块单板的温度或电压信息，如果没有输入该参数则查看当前所有正常上线的单板的温度或者电压信息。需要注意的是不同的单板上电压和温度的测量点个数可能不一样，通过命令查看某块单板的温度电压信息的时候也可以看到该单板测量点的阈值。主控上收集的上线单板温度电压信息会实时的与阈值比较，如果某块单板温度电压异常则会告警，告警的方法有两种，一种是日志，一种是蜂鸣，默认情况下只要有异常，主控的串口终端上会显示告警信息，并且蜂鸣器会产生蜂鸣，如果环境恢复正常那么主控的串口终端上会显示告警恢复信息并且停止蜂鸣器蜂鸣。蜂鸣是告警的可选方式，用户可以通过命令alarm enable,alarm disable来决定当环境异常的时候是否需要蜂鸣。

系统监控相关的命令如下表：

命令	描述	CLI模式
show temperature [slot-id]	显示系统的各个监测点的温度值。如果没有输入参数，显示系统的所有监测点的温度值，如果输入参数，显示指定的模块的监测点的温度值。	普通模式，特权模式
show voltage [slot-id]	显示系统的各个监测点的电压值。如果没有输入参数，显示系统的所有监测点的电压值，如果输入参数，显示指定的模块的监测点的电压值。	普通模式，特权模式
alarm enable	启动蜂鸣告警方式，当系统的温度或者电压异常时，系统的蜂鸣器会蜂鸣。	模块配置模式
alarm disable	关闭蜂鸣告警方式，当系统的温度或者电压异常时，系统的蜂鸣器不会蜂鸣。	模块配置模式
show running-config	查看系统的当前配置，可以查	特权模式

	看到蜂鸣告警方式的配置。	

下面是一个使用show temperature命令显示的内容的例子：

slotid	temp1	temp2	temp3	temp4
Mgta	33.5C（70.0C）	37.0C(70.0C)	40.C(70.0C)	NA
1	33.5C（70.0C）	37.0C(70.0C)	40.0C(70.0C)	42.0C(70.0C)

下面是一个使用show voltage命令显示的内容的例子：

slotid	voltage1	voltage2	voltage3	voltage4	voltage5	voltage6
Mgta	2.25 ~ 2.75	1.13~1.38	2.97~3.63	4.50~5.50	1.08~1.32	1.80~2.20
Mgta	2.50	1.23	3.23	4.97	1.19	1.99
1	2.25 ~ 2.75	1.13~1.38	2.97~3.63	1.80~2.20	10.80~13.20	1.08~1.32
1	2.50	1.24	3.27	2.00	12.13	1.20

2.4 配置文件管理

配置分为当前配置和初始配置两种。当前配置指的是系统运行时的配置，存在系统的内存中，而初始配置是系统启动时用到的配置，存在系统的FLASH中，也就是配置文件。当用户执行相关命令时修改的是系统的当前配置，只有执行了保存命令后才把当前配置写入到初始配置中，用于系统的下一次启动。当系统启动后用户在没有做任何配置的情况下，系统的当前配置信息与初始配置信息相同。

当前配置和初始配置采用相同的格式，都是命令行文本的格式，非常直观，便于用户阅读。配置文件的格式具有如下几个特点：

- 配置文件是文本文件。
- 保存的都是命令。
- 只保存非缺省的配置，对于缺省的配置不保存。
- 命令是按CLI模式来组织的，把同一个CLI模式下的命令组织在一起，形成一段，段与段之间以“!”隔开。对于全局配置模式内的命令，把同一功能或功能相近的命令组织成一段，以“!”隔开。
- 对于配置子模式内的命令，在命令前有一个空格，而对于全局配置模式内的命令，命令前不需要有空格。
- 以“end”作为配置的结束。

配置文件管理主要包括以下内容：

- 查看配置信息
- 保存配置
- 删除配置文件
- 配置文件上下载

2.4.1 查看配置信息

查看配置信息包括查看系统的当前配置和初始配置。初始配置实际上就是在FLASH中的配置文件，当FLASH中不存在配置文件时，系统启动时使用的是缺省配置，此时如果查看系统的初始配置，系统会提示配置文件不存在。

查看配置信息的命令如下表：

命令	描述	CLI模式
show running-config	查看系统的当前配置。	特权模式
show startup-config	查看系统的初始配置。	特权模式

2.4.2 保存配置

当用户修改了系统的当前配置，这些配置需要保存到配置文件中去，这样下一次启动后这些配置还依然存在，否则，重启后这些配置信息就丢失了。保存配置就是把当前配置保存到初始配置中。

保存配置的命令如下表：

命令	描述	CLI模式
write	保存当前的配置。	特权模式

注意：用户在对交换机做了配置后需要使用此命令保存配置，否则系统重启后配置会丢失。

2.4.3 删除配置文件

当用户希望系统的初始配置回到缺省配置时可以删除配置文件，删除配置文件后对当前配置没有影响，如果希望系统的当前配置回到缺省配置时，需要重启交换机。用户在做删除配置文件时一定要谨慎，否则配置会丢失。

删除配置文件的命令如下表，

命令	描述	CLI模式
delete startup-config	删除系统的配置文件。	特权模式

2.4.4 配置文件上下载

为了配置文件的安全性，用户可以使用命令把配置文件上载到PC机上做备份，当系统的配置异常丢失或做了修改后希望回到原来的配置时，可以从PC机上把原来的配置文件下载到交换机上，下载配置文件后对系统的当前配置没有影响，必须重启交换机后配置就能生效。

配置文件上下载的命令如下：

命令	描述	CLI模式
upload configure <ip-address> <file-name>	把配置文件上载到PC机上，第一个参数是PC机的IP地址，第二个参数是配置文件在PC机上存储的文件名。	特权模式
download configure <ip-address> <file-name>	把配置文件下载到PC机上，第一个参数是PC机的IP地址，第二个参数是配置文件在PC机上存储的文件名。	特权模式

配置文件上下载使用到TFTP协议，在交换机上运行TFTP客户端软件，在PC机上运行TFTP服务端软件。配置文件上下载的操作步骤如下：

第一步： 搭建网络环境

第二步： 在PC机上启动TFTP服务端软件，设置配置文件所存放的目录。

第三步： 在交换机上保存配置。

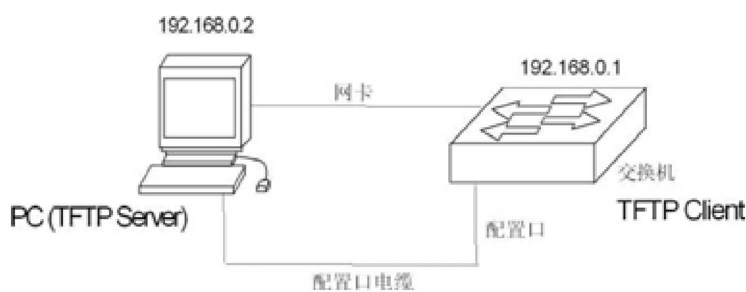
第四步： 在交换机上执行配置文件上载命令把配置文件备份到PC机上。

第五步：当交换机需要PC机上的配置文件时，在交换机上执行配置文件下载命令把PC机上的配置文件下载到交换机上。

第六步：要使配置生效，必须重启交换机。

示例： 一台已经配置好了VLAN和接口地址的交换机，需要进行配置文件上下载操作。

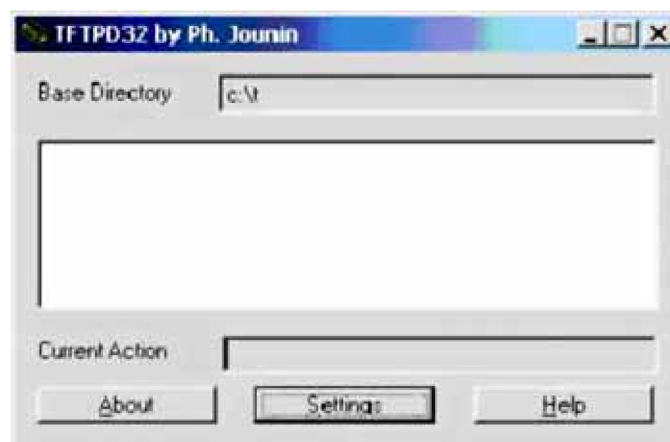
第一步： 搭建如下所示网络环境。



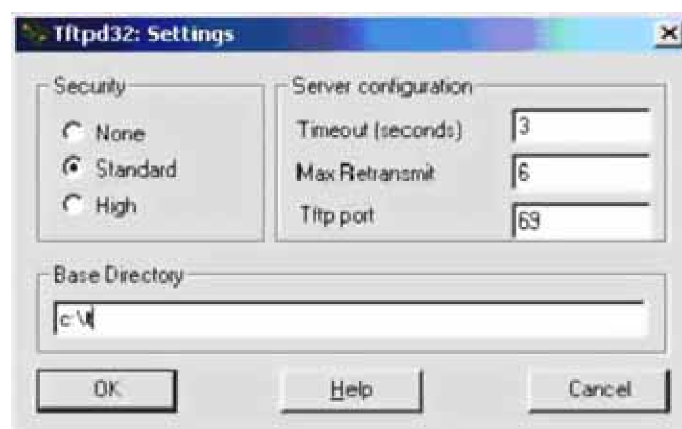
将交换机的配置口通过电缆外接一台配置终端，并通过网线与一台PC 相连。在PC 安装TFTP Server， 配置PC 的以太网口IP 地址，这里假定PC 的IP 地址为192. 168.0.2 。然后，配置交换机的IP 地址，这里假定交换机的IP 地址为192.168. 0 . 1 ，保证PC机与交换机之间的连通性。

第二步：启动TFTP Server，配置TFTP Server参数。

运行TFTP Server，窗口界面如下图：



然后，设置备份配置文件的目录。具体操作是，单击[Settings]按钮，设置界面，如下图：



在“Base Directory” 中输入文件路径。单击[OK]按钮确认。

第三步： 在交换机上执行write命令保存当前配置到配置文件中去。

第四步： 将文件备份到PC上，执行命令Switch#upload configuration 192.168.0.2 beifen.cfg。

第五步：必要时，将备份文件下载到交换机，执行命令Switch#download configuration 192.168.0.2 beifen.cfg。

第六步： 要想下载的配置文件能够生效，必须重启交换机，执行命令Switch#reset。

2.5 软件版本升级

iSpirit 8806交换机支持软件版本的在线升级。升级是通过工具TFTP来完成的。

2.5.1 联合文件

交换机在软件版本升级时使用的是联合文件。联合文件中包含管理模块和所有的接口模块的映像程序，是管理模块和接口模块的映像程序打包而形成的一个文件。用户在升级时只需要使用联合文件，在升级过程中系统会自动地更新管理模块和所有在位的接口模块的映像文件。

2.5.2 软件版本升级的命令

在全局配置模式下升级交换机的联合文件，命令如下：

download union <ip-address> <file-name>

其中<ip-address>为运行TFTP服务器的PC的IP地址，<file-name> 为在TFTP服务器上保存的联合文件名。

在升级的过程中不能断电，否则交换机的联合文件可能损坏而造成交换机启动不了。下载完毕后，需要重新启动交换机才能运行新下载的联合文件程序。整个升级过程需要几分钟，请您耐心等候。

在软件版本的升级过程中，系统会自动更新所有在位的接口模块的映像文件，此时不能重启交换机或断电，否则接口模块中的映像文件可能破坏，造成接口模块下一次启动不了。用户必须等到所有的接口模块都更新完毕后才能重启交换机或断电，在升级过程中在Console终端上有相应的提示。

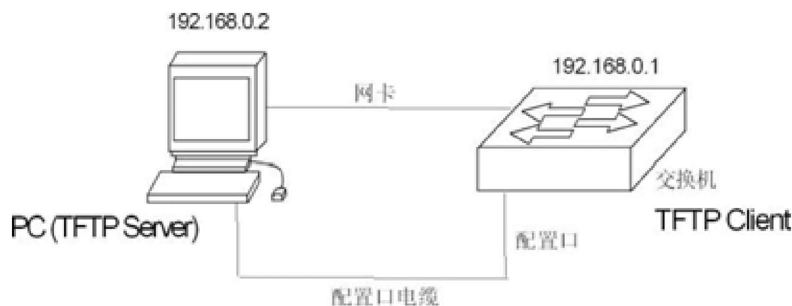
如果使用Telnet终端升级时要特别注意，在Telnet终端上升级完联合文件后会出现CLI提示符，但此时接口模块的映像文件还没有更新，在Telnet终端上也没有任何提示，用户最好在升级完联合文件后再等待几分钟再重启交换机或断电。

建议用户使用Console终端对交换机进行软件版本升级。

2.5.3 软件升级过程

升级联合文件步骤如下：

第一步：搭建升级环境。如下图所示。

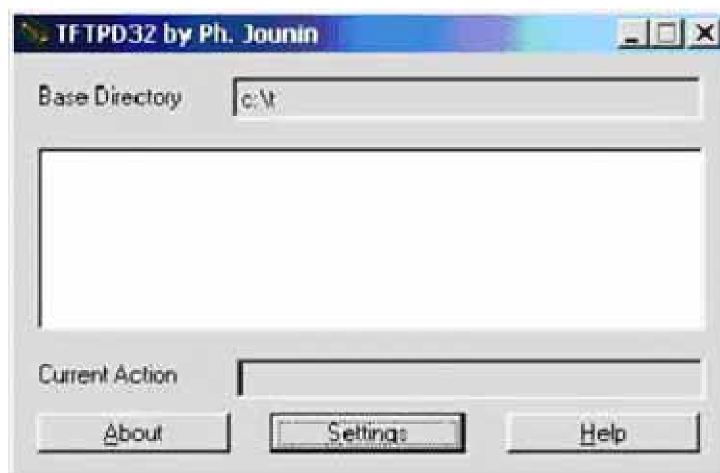


搭建过程如下：

- 将交换机的Console口通过电缆外接一台配置终端（PC）。
- 在PC上安装TFTP Server。
- 将新的联合文件拷贝到PC的某一路径下，这里假定路径为c:\t；
- 配置PC的以太网口IP 地址，这里假定PC的IP地址为192.168.0.2 。
- 配置交换机的IP地址，这里假定交换机的IP 地址为192.168.0.1。

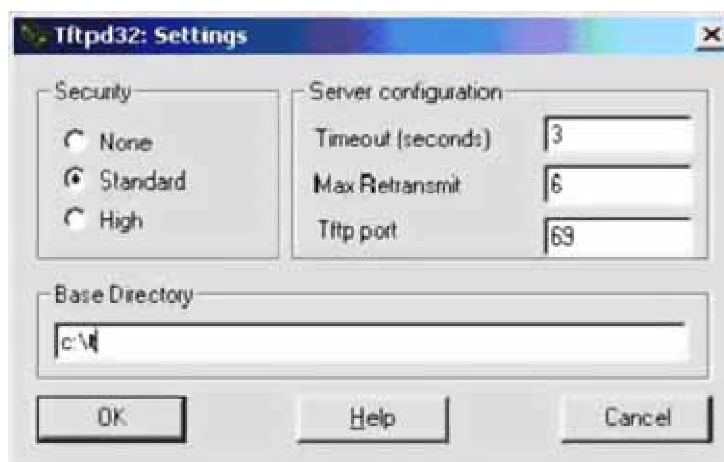
第二步：运行TFTP Server，并配置TFTP服务器。

首先： 运行TFTP Server 。TFTPD32 窗口界面如下图：



然后： 设置TFTP Server 文件目录。启动TFTP Server 之后，重新设置TFTP Server

文件目录，将待加载的联合文件拷贝到此目录之中。具体操作是，单击[Settings]按钮，出现TFTPD32 设置界面，如下图。



在“Base Directory” 中输入文件路径。单击[OK]按钮确认。

第三步：升级文件。

首先：将交换机的端口与运行TFTP Server 程序的PC通过以太网线连接。并用ping 命令检测主机与交换机之间是否连通。

然后：在超级终端Switch#提示符下输入命令：

Switch# download union 192.168.0.2 lenovo.uni，回车，等待升级联合文件完毕。

Loading…4136294

I am updating union,

Please wait and don’t shut me down…….

Updating union has completed !

I am updating master,

Please wait and don’t shut me down…….

Updating master has completed !

I am updating version,

Please wait and don’t shut me down…….

Updating version has completed !

I am updating Board(24gt) on slot 1,
Please wait and don’t shut me down…….

Board(24gt) on the slot 1 update has finished,
You should restart it !
Would you like to restart it ?(Y/N)y

I am updating Board(12gtt) on slot 2,
Please wait and don’t shut me down…….

Board(12gt) on the slot 2 update has finished,
You should restart it !
Would you like to restart it ?(Y/N)y
Switch#

注意：

交换机升级过程中，不能断电。

第四步： 重新启动交换机。

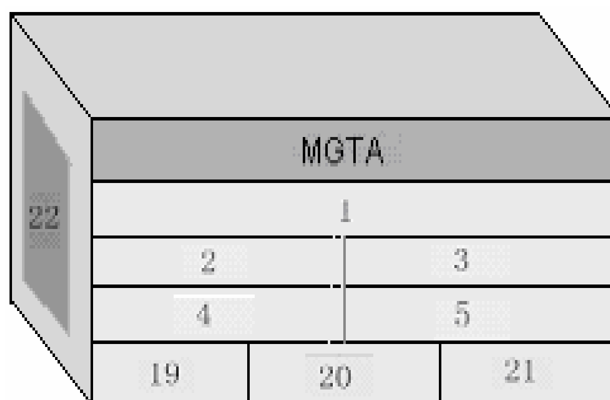
Switch# reset

第3章 配置模块

本章对模块相关的配置进行介绍（不包括增值业务模块，比如防火墙模块）。与模块相关的配置主要包括以下内容：

- 管理模块的自动配置
- 业务模块的自动配置
- 业务模块的手动配置
- 电源模块的自动配置
- 风扇模块的自动配置
- 管理模块，业务模块，电源模块，风扇模块信息查询
- 风扇模块故障自动告警
- 电源模块故障自动告警
- 业务模块不匹配自动告警
- 管理模块的主备倒换

iSpirit 8806交换机支持管理模块，业务模块（可插在1 2 3 4 5槽位），电源模块（可插在19 20 21槽）和风扇模块（可插在22槽位）的配置。其主要命令是完全兼容的。下面的图示说明了iSpirit 8806槽位分布。



iSpirit 8806 槽位分布图

3.1 管理模块的自动配置

交换机上电后，管理模块会自动启动自己的心跳，方便管理员查看管理模块运行是否正常，一般情况下，心跳正常表示管理模块正常，否则表示管理模块出现问题（此时如果存在主备两个管理模块而且当前模块为主用模块，则会发生主备倒换）。管理模块的心跳有两种查看方式：

- 通过模块信息查询命令查看管理模块心跳状态。
- 通过管理模块面板上的sys灯查看模块的心跳状态：sys灯闪烁表示模块心跳正常；sys灯常亮或者常灭表示模块心跳不正常。

交换机上电后，同时会自动检测管理模块的硬件在线状态。

3.2 业务模块的自动配置

交换机上电后，能够自动检测到交换机上插入的业务模块。交换机能识别插入的业务模块类别，并自动进行上线处理。业务模块的上线状态分为2个级别：

- 硬件在线（离线）：此种状态表示相应的槽位的硬件是否已经在位准备好
- 软件在线（离线）：此种状态表示相应槽位的业务模块软件是否已经准备好

注意：硬件在线不一定能保证软件在线，但软件在线一定要求硬件在线，下面的表格说明了可能出现的情况：

硬件在线状态	软件在线状态	说明
在线	在线	表示业务模块软硬件均已经准备好，可以进行相应的操作
在线	离线	此种状态可能在以下条件下出现： 业务模块已经插入相应槽位，正在进行软件上线的处理过程 业务模块已经插入相应槽位，但由于业务模块损坏导致软件启动不正常 业务模块已经插入相应槽位，但该槽位原来已经配置了另外一种类型的业务模块(用户手动配置或是从配置文件配置)（此种情况下会同时上报业务模块不匹配告警）。
离线	在线	正常情况下突然拔出业务模块，软件正在下线处理过程中会出现此种状态
离线	离线	业务模块没有插入相应槽位

业务模块的软硬件在线状态可以通过模块信息查询命令获得。

如果相应的槽位并没有插入模块，则手动创建的模块软硬件在线状态均为离线。业务模块自动上线时，将会通过log形式通知管理员，其上报内容如下：

参数名称	参数说明
Alm_type	消息类型，此处为BD_ONLINE：业务模块上线
Alm_level	消息重要级别，此处为5：很重要
message	其他信息： bd_type：自动配置的业务模块类型 slotid：业务模块槽位号

业务模块上线后，管理员手动拔除业务模块，交换机将会对业务模块自动进行下线处理，同时通过log形式通知管理员，其上报内容如下：

参数名称	参数说明
Alm_type	消息类型，此处为BD_OFFLINE：业务模块下线
Alm_level	消息重要级别，此处为5：很重要
message	其他信息： bd_type：自动下线的业务模块类型 slotid：业务模块槽位号

3.3 业务模块的手动配置

业务模块除了支持自动配置外，还支持用户手动进行配置，主要包括：

- 用户手动创建业务模块
- 用户手动删除业务模块

3.3.1 用户手动创建业务模块

下面的命令在模块配置模式下手动创建业务模块：

Switch(config-module)#create module <module-id> <module-type>

例如在槽位1上创建24GT模块：

Switch(config-module)#create module 1 24gt

其中：

槽位号module-id可以取1 2 3 4 5。

模块类型module-type为当前支持的模块，如下所示，以后还将支持新的模块。

模块名称	模块说明
24gt	24口千兆电口模块
24gx	24口千兆光口模块
10g2x	2口万兆光口模块

28xt	12口千兆光口+16口千兆电口模块
16xt	12口千兆光口+4口千兆电口模块
12gt	12口千兆电口模块

如果模块已经创建（或自动上线）并且模块类型和现在参数中的模块类型不相同，则返回失败，如果相同或原来槽位并没有创建（或自动上线）模块则返回成功。

3.3.2 用户手动删除业务模块

下面的命令在模块配置模式下手动删除业务模块：

Switch(config-module)#remove module <module-id>

例如删除槽位1上创建的24GT模块：

Switch(config-module)#remove module 1

其中：

槽位号module-id在iSpirit 8806中可以取1 2 3 4 5。

如果相应的槽位并没有模块，则返回失败。

如果相应的槽位存在模块而且硬件软件在线，删除后过一段时间此模块又会自动创建并自动上线。

3.4 电源模块的自动配置

交换机上电后，交换机会启动对电源模块的检测，并在电源出现故障时上报告警。电源状态的信息有两种方式获得：

- 通过模块信息查询命令获得电源模块在位，运行是否正常等状态。
- 通过面板上的PWR1 PWR2 PWR3灯查看三个电源的运行状态。灯常亮表示电源在线且运行正常，灯闪烁表示电源在线但运行不正常，灯不亮表示电源不在线。

3.5 风扇模块的自动配置

交换机上电后，交换机会启动对风扇模块的检测，并在风扇出现故障时上报告警。风扇状态的信息有两种方式获得：

- 通过模块信息查询命令获得风扇模块在位，运行是否正常等状态。
- 通过面板上的FAN灯查看风扇的运行状态。灯常亮表示风扇在线且运行正常，灯闪烁表示风扇在线但运行不正常，灯不亮表示风扇不在线。

3.6 管理模块，业务模块，电源模块，风扇模块信息查询

下面的命令在普通模式或特权模式下查询管理模块，业务模块，电源模块，风扇模块的运行状态：

Switch#show module [module-id]

例如查询槽位1上的业务模块信息如下：

Switch#show module 1

slotid	modulename	online	other
1	24gt	online	on /heartbeat

其中：槽位号module-id在iSpirit 8806中可以取1 2 3 4 5（业务模块）17（MGTA）19 20 21（电源模块）22（风扇模块）。

也可以查询所有模块的信息，只要不输入槽位号module-id参数就可以了，如下：

Switch#show module

slotid	modulename	online	other
0	mgt-12xt	online	on /heartbeat
1	24gt	online	on /heartbeat
2	null	offline	off/no heartbeat
3	null	offline	off/no heartbeat
4	null	offline	off/no heartbeat
5	null	offline	off/no heartbeat
17	mgt-a	online	master
19	power	online	null
20	power	offline	null
21	power	offline	null

22 fan online fail

查询返回的各参数说明如下：

参数名称	参数说明
slotid	槽位号
modulename	模块名称： mgt-12gt：主控卡上12口千兆电口板 24gt：24口千兆电口板 24gx：24口千兆光口板 10g2x：2口万兆光口板 28xt：12口千兆光口+16口千兆电口模块 16xt：12口千兆光口+4口千兆电口模块 12gt：12口千兆电口板 mgt-a：主控A槽 power：电源板 fan：风扇板
online	软件在线标志
other	业务模块：业务模块硬件是否在线/业务模块心跳是否正常 管理模块：管理模块主用备用状态/管理模块心跳是否正常 电源风扇：运行是否正常，fail表示运行不正常；warning表示存在告警

3.7 风扇模块故障自动告警

交换机上电后，交换机会启动对风扇模块的检测，当风扇模块出现故障时，交换机会自动上报告警，其内容包括：

参数名称	参数说明
Alm_type	告警类型，此处为FAN_WARN：风扇告警
Alm_level	告警级别，此处为5：严重故障

message	其他消息： slotid：模块槽位号，此处固定为22 brd_type：模块类型类型，此处固定为fan status：板状态，在线/离线，有告警时板状态後将有warning显示

交换机启动时风扇故障则上报告警一次，同时风扇由好变坏或由坏变好时上报告警。

3.8 电源模块故障自动告警

交换机上电后，交换机会启动对电源模块的检测，当电源模块出现故障时，交换机会自动上报告警，其内容包括：

参数名称	参数说明
Alm_type	告警类型，此处为POWER_WARN：电源告警
Alm_level	告警级别，此处为5：严重故障
Message	其他消息： slotid：电源模块槽位号 brd_type：模块类型类型，此处为power status：板状态，在线/离线，有告警时板状态後将有warning显示

交换机启动时电源故障则上报告警一次，同时任何一个电源模块由好变坏或由坏变好时上报告警。

3.9 业务模块不匹配自动告警

如果管理员手动创建了一个离线模块，然后在相应槽位插入了一个不匹配的模块，则交换机将上报业务模块不匹配告警。告警内容如下所示：

参数名称	参数说明
Alm_type	告警类型，此处为BD_NOMATCH：业务模块不匹配
Alm_level	告警级别，此处为5：严重故障
message	其他消息： slotid：业务模块槽位号 old_type：原来创建的业务模块类型 new_type：硬件实际插入的业务模块类型

发生此种告警时，此告警将每隔2秒一直上报，直到管理员干预，管理员可以拔除不匹配的业务模块或手动删除原来创建的业务模块来消除此告警。

第4章 配置端口

本章对端口相关的配置进行介绍，主要包括以下内容：

- 端口的通用配置
- 配置MIRROR
- 配置STORM-CONTROL
- 配置FLOW-CONTROL
- 配置端口带宽
- 配置TRUNK

4.1 端口的通用配置

管理员通过对交换机的端口配置控制端口下接入的用户，如不让端口下的用户接入网络，管理员可以关闭这个端口。本节对端口的通用配置进行介绍，主要包括：

- 端口的打开和关闭
- 端口的速率配置
- 显示端口的信息

4.1.1 端口的打开和关闭

iSpirit 8806交换机的端口缺省是打开的，如果管理员希望端口下的用户不能接入网络，可以关闭这个端口。

下面的命令在接口配置模式下打开端口的管理状态：

no shutdown

例如打开端口1/1的管理状态：

Switch(config-ge1/1)#no shutdown

下面的命令在接口配置模式下关闭端口的管理状态：

Shutdown

例如关闭端口1/1的管理状态：

Switch(config-ge1/1)#shutdown

4.1.2 端口的速率配置

所有的端口的缺省速率配置是自适应（autonegotiate）的。

下面的命令在接口配置模式下配置端口的速率：

speed {autonegotiate |full-1000 |full-100 |full-10 |half-100 |half-10 }

autonegotiate---自适应

full-1000-------全双工千兆

full-100--------全双工百兆

full-10 --------全双工十兆

half-100--------半双工百兆

half-10---------半双工十兆

例如端口1/1的速率配置成全双工1000M：

Switch(config-ge1/1)# speed full-1000

4.1.3 显示端口的信息

下面的命令在普通模式或特权模式下显示一个或多个端口的信息：

show interface [if-name]

例如显示端口1/1的信息：

Switch# show interface ge1/1

例如显示所有端口的信息：

Switch# show interface

4.2 配置 MIRROR

端口镜像对于监听一个或多个端口接收和发送的包的流量是一个非常有用的功能，它能用镜像端口去监听一个或多个端口的接收和发送的包。联想天工iSpirit 8806交换机支持端口镜像功能，镜像端口能够监听别的端口的进入的数据和出去的数据。一个镜像端口可以同时监听多个端口。本节重点介绍MIRROR 的配置，主要包括以下内容：

- 配置MIRROR的监听端口和被监听端口
- 显示MIRROR配置

4.2.1 配置 MIRROR 的监听端口和被监听端口

管理员配置监听端口的时候，需要进入此接口配置模式设置被监听端口，例如设置端口ge1/1监听端口ge1/2，则需要进入端口ge1/1下，键入命令：

Switch(config-ge1/1)# mirror interface ge1/2 direction both

此时，端口ge1/1被设置为监听端口，ge1/2被设置为被监听端口。

设置被监听端口的命令如下：

Switch(config-ge1/1)#mirror interface <if-name> direction {both | receive | transmit}

此时，端口ge1/1设置为监听端口，<if-name>设置为被监听端口，同时后面的{both | receive | transmit}指明了监听的方向：receive表示监听收到的数据包；transmit监听发送的数据包；both监听发送和接收的所有数据包。比如：

Switch(config-ge1/1)#mirror interface ge1/2 direction both

表示设置端口ge1/1监听端口ge1/2的发送和接收的数据包。

如果要设置多个被监听端口，需要执行多次命令。

管理员在接口配置模式下，可以取消被监听端口，命令如下：

Switch(config-ge1/1)#no mirror interface <if-name>

此时<if-name>是不再被监听的端口。比如：

Switch(config-ge1/1)# no mirror interface ge1/2

表示设置端口ge1/1不再监听端口ge1/2的数据包。

当所有被监听端口都被取消时，监听端口也将被清除。

4.2.2 显示 MIRROR 的配置

管理员可以在普通模式或特权模式下通过下面命令查看已经设置的MIRROR配置：

Switch# show mirror

需要注意以下几点：

- 一个端口不能同时设置为监听端口和被监听端口。
- 监听端口只能有一个，但被监听端口可以有多个。
- 交换机支持跨模块的端口监听功能。

4.3 配置 STORM-CONTROL

在现实生活中，一个NIC卡发很高速率的单播、组播、广播包可以使得网络出现故障，

在这种情况下，交换机上的抑制功能便显得尤为重要，它能防止数据包涌进网络而造成网络拥塞的情况，联想天工iSpirit 8806交换机的所有端口支持广播包、组播包和DLF 包的抑制功能。

本节对STORM-CONTROL的配置进行详细的描述，主要包括以下内容：

- 缺省配置
- 广播抑制配置
- 组播抑制配置
- DLF 抑制配置
- 显示STORM-CONTROL配置

4.3.1 缺省配置

iSpirit 8806交换机支持对每个端口分别设置broadcast rate, multicast rate, dlf rate 。默认端口的广播包抑制到1500个，目的是防止网络形成广播风暴。DLF包缺省抑制到1500个包，组播包缺省没有做抑制。

4.3.2 广播抑制配置

下面的命令在接口配置模式下配置此端口的广播抑制：

storm-control broadcast level <rate>

其中rate的范围为0.00–100.00，表示百分比。

下面的命令在接口配置模式下取消此端口的广播抑制的配置：

no storm-control broadcast level

4.3.3 组播抑制配置

下面的命令在接口配置模式下配置此端口的组播抑制：

storm-control multicast level <rate>

其中rate的范围为0.00–100.00，表示百分比。

下面的命令在接口配置模式下取消此端口的组播抑制的配置：

no storm-control multicast level

4.3.4 DLF 抑制配置

下面的命令在接口配置模式下配置此端口的DLF抑制：

storm-control dlf level <rate>

其中rate的范围为0.00–100.00，表示百分比。

下面的命令在接口配置模式下取消此端口的DLF抑制的配置：

no storm-control dlf level

4.3.5 显示 STORM-CONTROL 配置

下面的命令在普通模式或特权模式下显示STORM-CONTROL配置：

show storm-control

4.4 配置 FLOW-CONTROL

FLOW-CONTROL（流量控制）用于防止在端口阻塞的情况下数据丢包。在半双工方式下，流量控制通过背压（Backpressure）技术实现，使得信息源降低发送速率。在全双工模式下，流量控制遵循IEEE802.3x标准，阻塞端口向信息源发送“Pause”包令其暂停发送。

本节对FLOW-CONTROL（流量控制） 的配置进行详细的描述，主要包括以下内容：

- 缺省配置
- 设置端口发送侧流控
- 设置端口接收侧流控
- 关闭端口流控
- 显示流控信息

4.4.1 缺省配置

iSpirit 8806交换机支持对每个端口分别设置发送和接收的流控。默认端口并没有打开流控功能。

4.4.2 设置端口发送侧流控

下面的命令在接口配置模式下配置端口发送侧流控打开：

flowcontrol send on

下面的命令在接口配置模式下配置端口发送侧流控关闭：

flowcontrol send off

4.4.3 设置端口接收侧流控

下面的命令在接口配置模式下配置端口接收侧流控打开：

flowcontrol receive on

下面的命令在接口配置模式下配置端口接收侧流控关闭：

flowcontrol receive off

4.4.4 关闭端口流控

下面的命令在接口配置模式下关闭端口发送和接收侧流控：

no flowcontrol

4.4.5 显示流控信息

下面的命令在普通模式或特权模式下显示所有端口的流控信息：

show flowcontrol

下面的命令在普通模式或特权模式下显示某一个端口的流控信息：

show flowcontrol interface <if-name>

其中，<if-name>为要查询流控信息的端口名称。

4.5 配置端口带宽

端口带宽控制用于控制端口发送和接收的速率。

本节对端口带宽的配置进行详细的描述，主要包括以下内容：

- 缺省配置
- 设置端口发送或接收带宽控制
- 取消端口发送或接收带宽控制
- 显示端口配置的带宽控制

4.5.1 缺省配置

iSpirit 8806交换机支持对每个端口分别设置发送和接收的带宽。默认端口并没有进行带宽控制。

4.5.2 设置端口发送或接收带宽控制

下面的命令在接口配置模式下设置端口发送或接收带宽控制：

portrate {egress | ingress} <rate>

egress表示对发送的数据包进行带宽控制。

ingress表示对接收的数据包进行带宽控制。

<rate>表示要设置的带宽的值，范围为1－1048512，单位为kbits。

4.5.3 取消端口发送或接收带宽控制

下面的命令在接口配置模式下取消端口的带宽控制：

no portrate {egress | ingress}

egress表示取消发送数据包的带宽控制。

ingress表示取消接收数据包的带宽控制。

4.5.4 显示端口配置的带宽控制

下面的命令在普通模式或特权模式下查看端口配置的带宽控制：

show portrate interface <if-name>

其中<if-name>为要查询带宽控制信息的端口名称。

4.6 配置 TRUNK

TRUNK是把多个端口聚合成一个逻辑端口，它可以用来增加带宽，提供冗余备份连接，还可以用来负载均衡。TRUNK组作为输出逻辑端口时，交换机将会根据用户设置的聚合策略从端口组中选择一个端口将包发送出去。TRUNK组的端口和聚合策略的配置由软件来完成，但数据流的转发都是通过硬件来完成的。

TRUNK组中的所有端口必须配置为同样的速度，而且是全双工模式才行。iSpirit8806交换机可支持最多32组TRUNK，每组TRUNK成员最多可达8个。同组TRUNK中的各个端口可以跨模块。需要特别注意的是每一端口只能属于一个TRUNK组。

本节对TRUNK的配置进行详细的描述，主要包括以下内容：

- TRUNK组的配置
- TRUNK成员端口配置
- TRUNK负载均衡策略配置
- TRUNK的显示

4.6.1 TRUNK 组的配置

下面的命令在配置模式下创建一个TRUNK组：

trunk <trunk-id>

创建TRUNK组，<trunk-id>值范围是1-32，表示要创建的TRUNK组ID号，最多可配置32

组TRUNK；创建成功后该TRUNK组的接口名称为trunk+id号，如组ID号为1的TRUNK组的接口名为trunk1。可以在配置模式下用"interface trunk+id号"命令进入接口配置模式，再对TRUNK组进行操作，如使用命令interface trunk1进入TRUNK 1的接口模式，对TRUNK 1进行配置。

下面的命令在配置模式下删除一个TRUNK组：

no trunk <trunk-id>

删除TRUNK组时必须要保证该TRUNK组没有成员端口。

4.6.2 TRUNK 组成员端口配置

下面的命令在接口配置模式下新添TRUNK组成员端口：

trunk interface <if-name>

<if-name>是需要添加入TRUNK组的端口名称，必须为二层接口。每一组TRUNK最多可以添加8个二层接口。

下面的命令在接口配置模式下删除该TRUNK组所有成员端口：

no trunk interface

下面的命令在接口配置模式下删除指定TRUNK组成员端口：

no trunk interface <if-name>

可多次使用这个命令删除该TRUNK组的多个成员端口。

4.6.3 TRUNK 负载均衡策略配置

下面的命令在接口配置模式下设置端口的负载均衡策略：

trunk load-balance {dst-mac |dst-ip |src-dst-mac |src-dst-ip | src-mac |src-ip }

dst-mac--------基于目的MAC 的均衡策略

dst-ip------------基于目的IP 的均衡策略

src-dst-mac---基于源MAC 和目的MAC 的均衡策略

src-dst-ip -----基于源IP 和目的IP 的均衡策略

src-mac--------基于源MAC 的均衡策略

src-ip------------基于源IP 的均衡策略

下面的命令在接口配置模式下设置默认的端口负载均衡策略：

no trunk load-balance

默认的端口负载均衡策略是src-dst-mac（基于源和目的MAC的均衡策略）。

4.6.4 TRUNK 的显示

下面的命令在普通模式或特权模式下查看所有TRUNK组配置：

show trunk

下面的命令在普通模式或特权模式下查看指定TRUNK组配置：

show trunk <trunk-id>

其中<trunk-id>为要查询的TRUNK组的ID号。

第5章 配置VLAN

VLAN 是交换机中的一个重要概念，在实际应用中使用非常多，它是内部划分多个网络的基础。VLAN 是虚拟局域网的简称，它是逻辑地把多个设备组织在一起的一个网络，而不管设备的物理位置在哪里。每个VLAN 都是一个逻辑网络，它具有传统的物理网络的一切功能和属性。每个VLAN都是一个广播域，广播包只能在一个VLAN 内进行转发，不能跨越VLAN，VLAN间的数据通信必须通过三层转发。

本章主要包括以下内容：

- VLAN 介绍
- VLAN 配置
- VLAN 配置示例

5.1 VLAN 介绍

本节对VLAN 进行一个详细的介绍，主要包括以下内容：

- VLAN 的好处
- VLAN ID
- VLAN 端口成员类型
- 端口的缺省VLAN
- 端口的VLAN模式
- VLAN 中继
- 数据流在VLAN 内的转发
- VLAN 的子网

5.1.1 VLAN 的好处

VLAN 极大地扩展了物理网络的规模。传统的物理网络只能有一个很小的规模，最多能容纳上千台设备，而使用VLAN 划分的物理网络能够容纳上万甚至几十万台设备。VLAN 与传统的物理网络有相同的功能和属性。

使用VLAN 有以下好处：

- VLAN 能有效控制网络中的流量。

在传统网络中，不管有无必要，所有的广播包都传送到所有的设备，加重了网络和设备的负载。而VLAN 能够根据需要把设备组织在一个逻辑网络中，一个VLAN 就是一个广播域，广播包只在VLAN 内部传送，不会跨越VLAN 。通过划分VLAN 可以有效地控制网络中的流量。

- VLAN 能够提高网络的安全性。

VLAN 内的设备只能与同一个VLAN 的设备进行二层通信，如果要与另一个VLAN 通信，必须通过三层转发，如果不建立VLAN 间的三层转发，VLAN 间完全不能通信，可以起到隔离的作用，保证每个VLAN 内的数据安全。例如一个公司研发部不想与市场部的数据进行共享，可以研发部建立一个VLAN， 市场部建立一个VLAN， 二个VLAN 间不建立三层通信通道。

- VLAN 使设备的移动变得方便。

传统的网络中的设备如果从一个位置移动到另一个位置而属于不同的网络时，需要修改移动

设备的网络配置，这样对于用户来说是非常不方便的。而VLAN 是一个逻辑网络，可以把不在同一物理位置的设备划在同一个网络，当设备移动时还可以使设备属于此VLAN 中，这样移动的设备不需要修改任何配置。

5.1.2 VLAN ID

每一个VLAN 有一个标识号，叫VLAN ID，VLAN ID 的范围从0 到4095，其中0 和4095 不用，实际有效的只有1 到4094 。VLAN ID 唯一标识一个VLAN 。

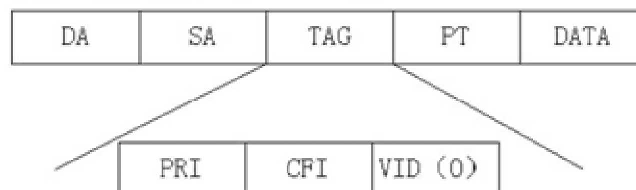
iSpirit 8806交换机支持4094 个VLAN ，在创建VLAN 时，要选择一个VLAN ID ，范围从2到4094。交换机在缺省情况下创建了VLAN1，并且VLAN1是不能被删除的。

在网络中的一个VLAN 内传输的数据帧有三种： 不带标记的数据帧，带VID 为0 的标记的数据帧，带VID 非0 的标记的数据帧。如下图所示为三种不同数据帧格式。

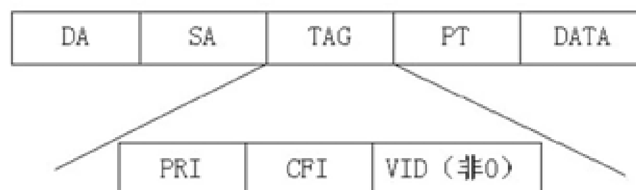
不带标记的数据帧



带标记的数据帧，但VLAN ID为0



带标记的数据帧，但VLAN ID非0



在交换机内部所有的数据帧都是带标记的。如果一个不带标记的数据帧输入交换机，交换机要给该数据帧加上一个标记，选择一个VLAN ID 值填入标记的VID 中。如果一个带VID 为0 的标记的数据帧输入交换机，交换机选择一个VLAN ID 值填入标记的VID 中。如果一个带VID 非0 的标记的数据帧输入交换机，该帧不变。

5.1.3 VLAN 端口成员类型

交换机支持基于端口的VLAN 和基于802.1Q 的VLAN 。一个VLAN 包括两种端口成员类型：untagged 成员和tagged 成员。一个VLAN 可以既包括untagged 端口成员，又包括tagged 端口成员。

一个VLAN 可以没有端口成员，也可以有一个或多个端口成员。当一个端口属于一个VLAN 时，可以是VLAN 的untagged 成员或tagged 成员。

一个端口可以属于一个或多个VLAN 的tagged或untagged成员，如果一个端口属于两个或多个VLAN 的tagged成员时，这个端口又称为VLAN 中继端口。一个端口可以同时属于一个或多个VLAN 的untagged 成员和属于另外的一个或多个VLAN 的tagged 成员。

5.1.4基于 MAC 的 VLAN 和基于 IP 子网的 VLAN

基于MAC的VLAN是根据数据包的源MAC地址来划分VLAN。它实现的机制是当一个不带VLAN标记或者VLAN标记的VLANID为0的数据包进入交换机时，交换机会根据用户在交换机上配置的MAC地址和VLANID的对应规则来决定这个数据包的VLANID。

基于IP子网的VLAN是根据数据包的源IP地址来划分VLAN。它实现的机制是当一个不带VLAN标记或者VLAN标记的VLANID为0的数据包进入交换机时，交换机会根据用户在交换机上配置的IP子网和VLANID的对应规则来决定这个数据包的VLANID。

这两种划分VLAN标记的好处是用户从一个地方移动到另外的地方访问网络时不需要重新划分VLAN和子网。

当交换机同时配置了基于MAC的VLAN和基于子网的VLAN时，基于MAC地址的VLAN优先生效。当一个不带标记或者VLAN标记为0的数据包既不能满足基于MAC的VLAN和基于IP子网的VLAN规则时，它的VLAN标记取决于输入端口的缺省VLAN。

5.1.5 端口的缺省 VLAN

端口有且只有一个缺省VLAN，缺省VLAN用于决定从该端口输入的不带标记或带标记但VID为0的数据包的所属VLAN。缺省VLAN又被称为端口VID或PVID。缺省情况下，端口的缺省VLAN为1。

5.1.6 端口的 VLAN 模式

端口存在三种VLAN模式：ACCESS模式，TRUNK模式和HYBRID模式。用户进行端口的VLAN配置时必须首先指定端口的VLAN模式。

ACCESS模式的端口是一个接入端口，直接面向用户，该端口只能属于一个VLAN的untagged成员，缺省VLAN是用户指定的VLAN。当端口只属于一个VLAN的untagged成员时，可以指定该端口的VLAN模式为ACCESS模式。

TRUNK模式的端口是一个中继端口，直接与交换机相连，该端口可以属于一个或多个VLAN的tagged成员，但不能属于任何VLAN的untagged成员，该端口的缺省VLAN为1，不能改变。

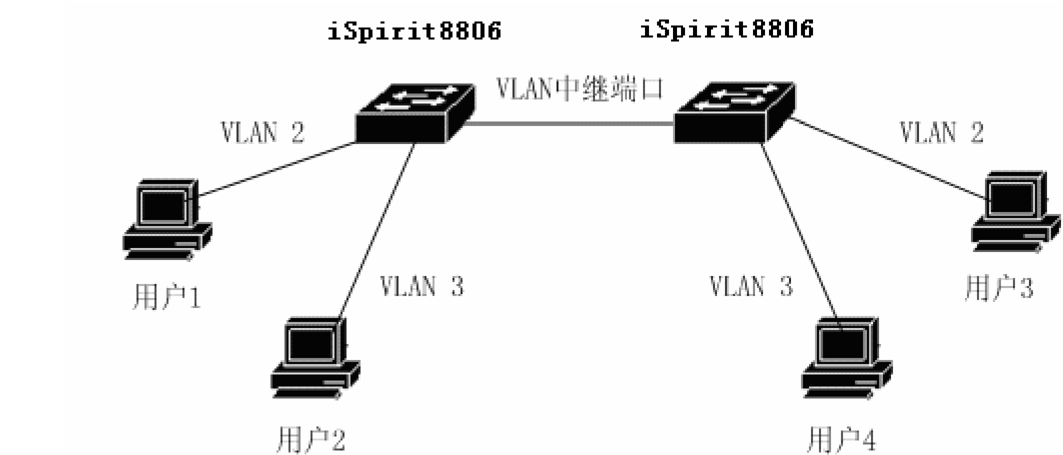
HYBRID模式的端口是一个中继端口，直接与交换机相连，该端口可以属于一个或多个VLAN的tagged成员和（或）一个或多个VLAN的untagged成员。该端口的缺省VLAN可以改变。

在实际应用时，用户可以根据具体情况来选择端口的VLAN模式。

5.1.7 VLAN 中继

如果一个端口属于两个或多个VLAN 的tagged成员，那么这个端口又称为VLAN 中继端口。两个交换机之间可以以VLAN 中继端口相连，这样两个交换机之间可以划分两个或多个共同的VLAN 。

如下图 是一个VLAN 中继的例子，两个交换机之间以VLAN 中继端口相连，是VLAN 2和VLAN 3 的中继端口，每个交换机划分为两个VLAN， 分别是VLAN 2 和VLAN 3， 每个VLAN 内有一个用户。这样，用户1 可以与用户3 通信，用户2 可以与用户4 通信，用户1 和用户3 不能与用户2 和用户4 通信。



5.1.8 数据流在 VLAN 内的转发

当交换机从一个端口收到一个数据包时，根据以下步骤进行二层转发：

- 决定该数据包所属的VLAN 。
- 判断该数据包是广播数据包、组播数据包还是单播数据包。
- 根据不同的数据包确定输出端口（可以是零个、一个或多个输出端口）， 如果没有输出端口，丢弃该数据包。
- 根据输出端口在VLAN 内的成员类型决定发出去的包是否带标记。
- 从输出端口发送出去。

1) 如何决定数据包的所属VLAN：

如果收到的数据包带标记并且标记中的VID 字段非0时，该数据包所属的VLAN 就是标记中V I D 值。

如果收到的数据包不带标记或带标记但标记中的VID 值为0时，该数据包所属的VLAN是端口的缺省VLAN。

2) 如何确定数据包的类型：

如果收到的数据包的目的MAC 地址是FF:FF:FF:FF:FF:FF，则该数据包是广播数据包。

如果收到的数据包不是广播数据包且其目的MAC 地址的第40 位为1，则该数据包是组播数据包。

如果既不是广播数据包又不是组播数据包，则该数据包为单播数据包。

3) 如何决定数据包的输出端口：

如果输入的数据包是广播数据包，该数据包所属的VLAN 的所有成员端口就是数据包的输出端口。

如果输入的数据包是组播数据包，首先根据目的组播MAC 地址和所属的VLAN 查找二层硬件组播转发表，如果找到匹配的组播条目，则组播条目中的输出端口和所属VLAN 中的成员端口中的共同端口（与操作）为数据包的输出端口，如果没有共同的端口，该数据包丢弃。如果在二层硬件组播转发表中没有找到匹配的组播条目，根据二层硬件组播转发表的转发模式决定输出端口，如果是未注册组播转发模式，组播包当作广播处理，所属的VLAN 的所有成员端口就是数据包的输出端口，如果是注册转发模式，则没有输出端口，数据包丢弃。

如果输入的数据包是单播数据包，首先根据目的MAC 地址和所属的VLAN 查找二层硬件转发表，如果找到匹配的条目，则条目中的输出端口与所属VLAN 的成员端口中的共同端口（与操作）为数据包的输出端口，如果没有共同的端口，该数据包丢弃。如果在二层硬件转发表中没有找到匹配的条目，该数据包当作广播包处理，所属的VLAN 的所有成员端口就是数据包的输出端口。

4) 发送数据包：

决定了输入的数据包的输出端口后要把数据包从所有的输出端口发送出去。

如果某个输出端口是数据包所属的VLAN 的untagged 成员，则数据包从该输出端口发送出去时不带标记。

如果某个输出端口是数据包所属的VLAN 的tagged 成员，则数据包从该输出端口发送出去时带标记，标记中的VID 值是数据包所属的VLAN 的值。

5.1.9 VLAN 的子网

在交换机上一个VLAN 是一个广播域， 一个VLAN 上可以建立一个子网接口，所有的子网都是建立在VLAN 的基础上的。iSpirit 8806交换机上最多可划分4094 个VLAN， 但最多只能建立512 个子网，当在512 个VLAN 上建立了子网后，其它的VLAN 就不能建立子网接口。子网接口的创建和删除不需要用户的干预，是系统自动完成的，当用户创建一个VLAN时，该VLAN对应的子网接口自动建立，当用户删除一个VLAN时，该VLAN对应的子网接口也被删除。

5.2 VLAN 配置

本节对VLAN 的配置进行详细的介绍，主要包括以下内容：

- 创建和删除VLAN
- 配置端口的VLAN模式
- ACCESS模式的VLAN配置
- TRUNK模式的VLAN配置
- HYBRID模式的VLAN配置
- 查看VLAN的信息

5.2.1 创建和删除 VLAN

在创建和删除VLAN之前，用户需要在全局配置模式下使用vlan database命令进入VLAN配置模式，在该模式下创建和删除VLAN。

系统在缺省情况下已经创建了VLAN 1，并且VLAN 1不能被用户删除。创建和删除VLAN的命令如下表：

命令	描述	CLI模式
vlan <vlan-id>	创建一个VLAN。如果该VLAN已经存在，则不做处理，否则创建此VLAN。参数的范围从2到4094。	VLAN配置模式
no vlan <vlan-id>	删除一个VLAN，如果该VLAN不存在，则不做处理，否则删除此VLAN。参数的范围从2到4094。	VLAN配置模式

5.2.2 配置端口的 VLAN 模式

在配置端口的VLAN之前需要指定端口的VLAN模式，缺省情况下端口的VLAN模式是

ACCESS模式。指定端口的VLAN模式的命令如下表：

命令	描述	CLI模式
switchport mode access	指定端口的VLAN模式是ACCESS模式。执行此命令后端口是VLAN1的untagged成员，端口的缺省VLAN是1。	接口配置模式
switchport mode trunk	指定端口的VLAN模式是TRUNK模式。执行此命令后端口是VLAN1的tagged成员，端口的缺省VLAN是1。	接口配置模式
no switchport trunk	端口的VLAN模式不再是TRUNK模式，回到缺省的情况，即ACCESS模式。	接口配置模式
switchport mode hybrid	指定端口的VLAN模式是HYBRID模式。执行此命令后端口是VLAN1的untagged成员，端口的缺省VLAN是1。	接口配置模式
no switchport hybrid	端口的VLAN模式不再是HYBRID模式，回到缺省的情况，即ACCESS模式。	接口配置模式

5.2.3 ACCESS 模式的 VLAN 配置

端口做VLAN配置之前需要指定端口的VLAN模式为ACCESS模式。在这种VLAN模式下端口缺省是VLAN1的untagged成员，端口的缺省VLAN是1。ACCESS模式的VLAN配置命令如下表：

命令	描述	CLI模式
switchport access vlan <vlan-id>	配置端口是指定的VLAN的untagged成员，端口的缺省VLAN是指定的VLAN。参数	接口配置模式

	范围从2到4094。	
no switchport access vlan	端口的VLAN配置回到缺省情况，即端口是VLAN1的untagged成员，端口的缺省VLAN是1。	接口配置模式

5.2.4 TRUNK 模式的 VLAN 配置

端口做VLAN配置之前需要指定端口的VLAN模式为TRUNK模式。在这种VLAN模式下端口缺省是VLAN1的tagged成员，端口的缺省VLAN是1。TRUNK模式的VLAN配置命令如下表：

命令	描述	CLI模式
switchport trunk allowed vlan all	配置端口是所有VLAN的tagged成员，对于以后新创建的VLAN，该端口也是这些VLAN的tagged成员。	接口配置模式
switchport trunk allowed vlan none	除VLAN1外，该端口不再是所有的其它VLAN的tagged成员。	接口配置模式
switchport trunk allowed vlan add <vlan-list>	配置端口成为指定的一个或多个VLAN的tagged成员。参数<vlan-list>可为一个VLAN、一个VLAN范围或多个VLAN。例如参数可以为“1”、“2-4”或“1,3,5”。	接口配置模式
switchport trunk allowed vlan remove <vlan-list>	把端口从指定的一个或多个VLAN中清除，不再是这些VLAN的tagged成员。参数<vlan-list>可为一个VLAN、一个VLAN范围或多个	接口配置模式

	VLAN。例如参数可以为“1”、“2-4”或“1,3,5”。	

5.2.5 HYBRID 模式的 VLAN 配置

端口做VLAN配置之前需要指定端口的VLAN模式为HYBRID模式。在这种VLAN模式下端口缺省是VLAN1的untagged成员，端口的缺省VLAN是1。HYBRID模式的VLAN配置命令如下表：

命令	描述	CLI模式
switchport hybrid vlan <vlan-id>	配置端口是指定的VLAN的untagged成员并且端口的缺省VLAN是指定的VLAN。参数范围从2到4094。	接口配置模式
no switchport hybrid vlan	把端口从缺省VLAN中清除，不再是缺省VLAN的tagged或untagged成员，端口的缺省VLAN回到1。	接口配置模式
switchport hybrid allowed vlan all	配置端口是所有VLAN（VLAN1除外）的tagged成员，对于以后新创建的VLAN，该端口也是这些VLAN的tagged成员。	接口配置模式
switchport hybrid allowed vlan none	除VLAN1外，该端口不再是所有的其它VLAN的tagged或untagged成员，端口的缺省VLAN回到1。	接口配置模式
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	配置端口成为指定的一个或多个VLAN的tagged成员。参数<vlan-list>可为一个VLAN、一个VLAN范围或多	接口配置模式

	个VLAN。例如参数可以为“1”、“2-4”或“1,3,5”。	
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	配置端口成为指定的一个或多个VLAN的untagged成员。参数 <vlan-list> 可为一个VLAN、一个VLAN范围或多个VLAN。例如参数可以为“1”、“2-4”或“1,3,5”。	接口配置模式
switchport hybrid allowed vlan remove <vlan-list>	把端口从指定的一个或多个VLAN中清除，不再是这些VLAN的tagged或untagged成员。如果端口的缺省VLAN属于指定的VLAN，则缺省VLAN回到1。	接口配置模式

5.2.6 查看 VLAN 的信息

查看VLAN的信息的命令如下表：

命令	描述	CLI模式
show vlan [vlan-id]	如果不输入参数，显示所有的VLAN信息，如果输入参数，显示指定的一个VLAN信息。参数范围从1到4094。	普通模式，特权模式
show interface switchport	显示系统的所有端口的VLAN相关信息，如VLAN模式，缺省VLAN等。	普通模式，特权模式
show running-config	查看系统当前配置，可以查看到VLAN的配置。	特权模式

5.2.7基于 MAC 的 VLAN 和基于 IP 子网的 VLAN 配置

基于MAC的VLAN和基于子网的VLAN配置不针对某个端口而是全局配置，也就是说只要配置了基于MAC的VLAN或者基于子网的VLAN对应规则，这些规则对交换机的所有端口都生效。

在配置基于MAC的VLAN时，分为三个步骤，先要配置MAC地址和VLANID的对应规则，然后把配置的规则加入到一个规则组，最后激活一个规则集合组。MAC地址和VLANID的对应关系规则ID的范围是129－1152，一共可以配置1024组。

在配置基于IP子网的VLAN时，和基于MAC的VLAN一样分为三个步骤，先要配置IP子网和VLANID的对应规则，然后把配置的规则加入到一个组，最后激活一个规则集合组。基于IP子网的VLAN的对应关系规则ID的范围是1-128，一个可以配置128组。

要注意的是规则可以配置多条，规则组也可以配置多个但是，基于MAC的VLAN和基于子网的VLAN规则同时可以加入到一个规则组，但是一个时刻只能激活的一个规则组。基于MAC地址和基于IP子网的VLAN的划分只是对没有VLAN标记或者VLAN标记为0的数据包生效，对于数据包已经包含非0的VLANID的数据包是不生效的。另外基于MAC地址和基于IP子网的VLAN的划分只是对进入交换机的数据包分配VLANID，并不对从这个出去的端口自动划分VLAN，因此还要配置需要移动的端口，并把这些端口划分为到所有基于MAC地址和基于IP子网VLAN的规则所涉及的VLAN中。

命令	描述	CLI模式
vlan classifier rule mac <129-1152> <mac-address> vlan <vlan-id>	配置基于MAC的VLAN规则	全局配置模式
vlan classifier rule ip <1-128> <ip-prefix> vlan <vlan-id>	配置基于IP的VLAN规则	全局配置模式
vlan classifier group <1-16> <add rule <1-1152>	把规则加入到一个组	全局配置模式
vlan classifier group <1-16> <delete> rule <1-1152>	从一个组中删除一条规则	全局配置模式
vlan classifier activate <1-16>	激活一个组	全局配置模式
show vlan classifier rule	显示配置的规则	特权模式

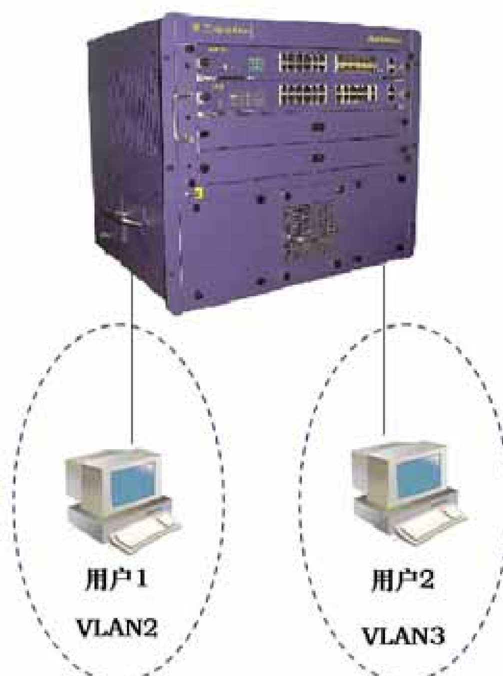
[1-1152]		
show vlan classifier group[1-16]	显示组	特权模式
show vlan classifier activation group <1-16>	显示当前激活的组	特权模式

5.3 VLAN 配置示例

5.3.1 基于 PORT 的 VLAN

1) 配置

有两个用户，用户1和用户2， 两个用户由于所使用的网络功能和环境不同，需要分别处于不同的VLAN中。用户1属于VLAN2，连接交换机的端口ge1/1，用户2属于VLAN3，连接交换机的端口ge1/2。



交换机的配置如下：

创建VLAN

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
```

将端口分配到VLAN中

```
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#swithport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#swithport mode access
Switch(config-ge1/2)#switchport access vlan 3
```

2) 排错

如果配置后，发现不同VLAN 之间的PC 机不能通信，那是正常现象，因为不同VLAN 之间要进行通信，必须要经过三层的路由转发。如果同一VLAN 内的PC 机不能进行通信，须作以下验证：

show vlan

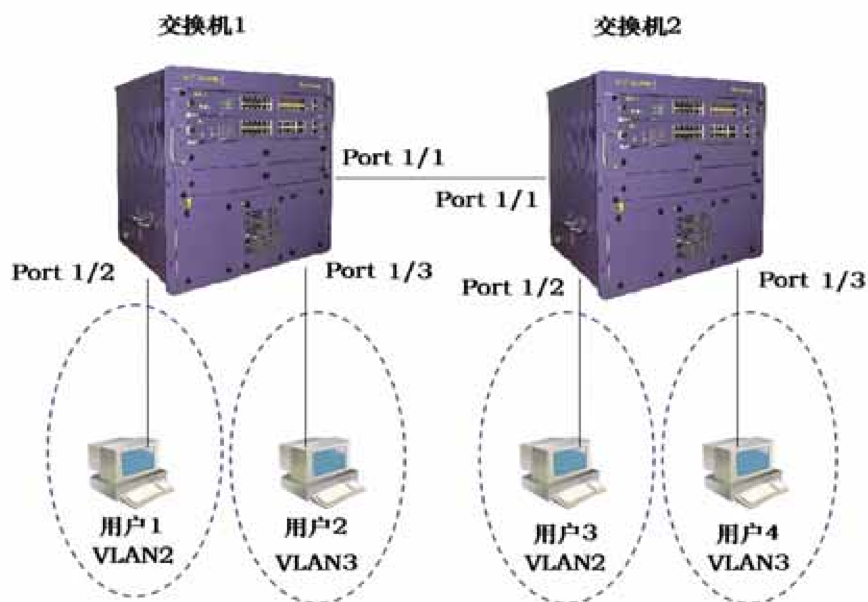
查看所有的VLAN的成员端口情况

show vlan <vlan-id>

查看连接特定PC机的端口是否在指定的VLAN内

5.3.2 基于 802.1Q 的 VLAN

1) 配置



有两台交换机分别连接两个用户：

用户	所属VLAN	连接端口	所属交换机	级联端口
用户1	2	1/2	交换机1	1/1
用户2	3	1/3	交换机1	1/1
用户3	2	1/2	交换机2	1/1
用户4	3	1/3	交换机2	1/1

需要在两台交换机上做配置。

交换机1配置：

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2
Switch(config-ge1/2)#swithport mode access
```

Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#swithport mode access
Switch(config-ge1/3)#switchport access vlan 3

交换机2配置：

Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2
Switch(config-ge1/2)#swithport mode access
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#swithport mode access
Switch(config-ge1/3)#switchport access vlan 3

2) 排错

跨交换机的vlan，在同一个vlan内的pc机都能够通信的，如果不能。须查看如下：

- 连接pc 机的端口是否属于相应的VLAN，且应用ACCESS模式加入这个vlan 的。
- 级联端口1/1是加入到每一个vlan中的，并且端口1/1是TRUNK模式。

5.3.3基于 MAC 的 VLAN 和基于 IP 子网的 VLAN

在交换中配置MAC为00:11:22:33:44:55的移动VLAN ID为3，192.168.3.1/24的VLAN ID为5。要移动的端口包括ge1/3, ge1/4, ge1/8。

Switch#configure terminal

配置基于IP子网的VLAN规则

Switch(config)#vlan classifier rule ipv4 1 192.168.3.1/24 vlan 5

配置基于MAC的VLAN规则

Switch(config)#vlan classifier rule mac 129 0011.2233.4455 vlan 3

把规则加入组集合

Switch(config)#vlan classifier group 1 add rule 1

Switch(config)#vlan classifier group 1 add rule 129

激活一个组

Switch(config)#vlan classifier activate 1

显示规则

Switch#show vlan classifier rule

vlan classifier rule ipv4 1 192.168.3.1/24 vlan 5

vlan classifier rule mac 129 011.2233.4455 vlan 3

显示组

Switch#show vlan classifier group

vlan classifier group 1 add rule 1

vlan classifier group 1 add rule 129

显示激活的组

Switch#show vlan classifier activation group

vlan classifier activate 1

配置VLAN

Switch#configure terminal

Switch(config)#vlan database

Switch(config-vlan)#vlan 3

Switch(config-vlan)#vlan 5

Switch(config-vlan)#exit

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode hybrid

Switch(config-ge1/3)#switchport hybrid allowed vlan add 3,5 egress-tagged disable

Switch(config-ge1/3)#interface ge1/4

Switch(config-ge1/4)#switchport mode hybrid

Switch(config-ge1/4)#switchport hybrid allowed vlan add 3,5 egress-tagged disable

Switch(config-ge1/4)#interface ge1/8

Switch(config-ge1/8)#switchport mode hybrid

```
Switch(config-ge1/8)#switchport hybrid allowed vlan add 3,5 egress-tagged disable
Switch(config-ge1/8)#end
Switch#show vlan
 VLAN   Name       State        Member ports ([u]-Untagged, [t]-Tagged)
 ----   --------   ---------    ------------------------------------------------
 1      vlan1      active       [u]ge0/1 [u]ge0/2 [u]ge0/3 [u]ge0/4 [u]ge0/5
                                 [u]ge0/6 [u]ge0/7 [u]ge0/8 [u]ge0/9 [u]ge0/10
                                 [u]ge0/11 [u]ge0/12 [u]ge1/1 [u]ge1/2 [u]ge1/3
                                 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9
                                 [u]ge1/10   [u]ge1/11 [u]ge1/12 [u]ge1/13 [u]ge1/14
                                 [u]ge1/15 [u]ge1/16 [u]ge1/17 [u]ge1/18 [u]ge1/19
                                 [u]ge1/20 [u]ge1/21 [u]ge1/22 [u]ge1/23 [u]ge1/24
 3      vlan3      active       [u]ge1/3 [u]ge1/4 [u]ge1/8
 5      vlan5      active       [u]ge1/3 [u]ge1/4 [u]ge1/8
```

第6章 配置QinQ

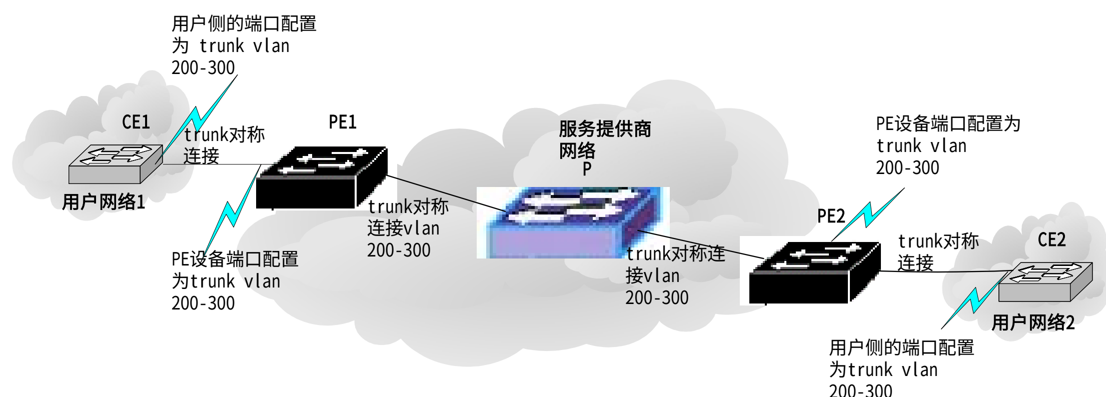
本章主要包括以下内容：

- QinQ 介绍
- QinQ 配置
- QinQ 配置示例

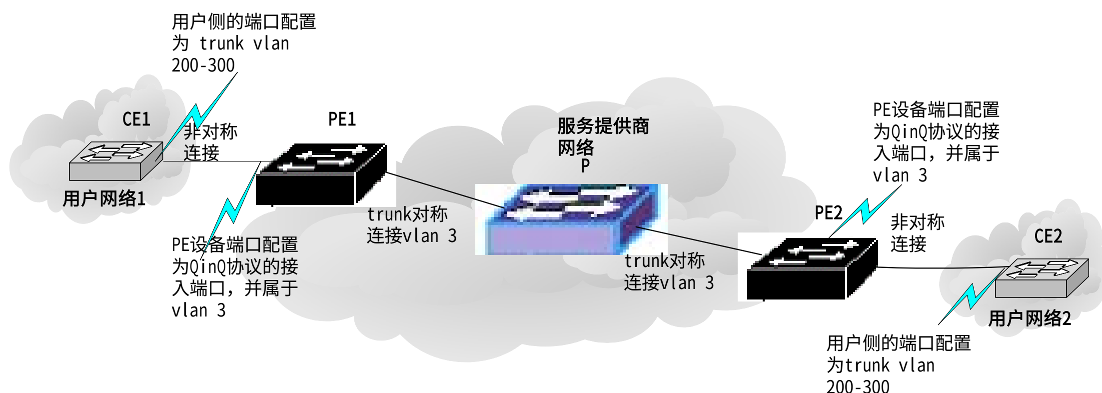
6.1 QinQ 介绍

QinQ是对802.1Q的扩展，其核心思想是将用户私网VLAN tag封装到公网VLAN tag上，报文带着两层tag穿越服务商的骨干网络，从而为用户提供一种较为简单的二层VPN隧道。其特点是简单而易于管理，不需要信令的支持，仅仅通过静态配置即可实现，特别适用于小型的，以三层交换机为骨干的企业网或小规模城域网。

下图为基于传统的802.1Q协议的网络，假设某用户的网络1和网络2位于两个不同地点，并分别通过服务提供商的PE1、PE2接入骨干网，如果用户需要将网络1的VLAN200-300和网络2的VLAN200-300互联起来，那么必须将CE1、PE1、P和PE2、CE2的相连端口都配置为Trunk属性，并允许通过VLAN200-300，这种配置方法必须使用户的VLAN在骨干网络上可见，不仅耗费服务提供商宝贵的VLAN ID资源（一共只有4094个VLAN ID资源），而且还需要服务提供商管理用户的VLAN号，用户没有自己规划VLAN的权利。



为了解决上述问题，QinQ协议向用户提供一个唯一的公网VLAN ID，这个特殊的VLAN ID被称作SP-ID，将用户私网VLAN tag封装在这个新的SP-ID中，依靠它在公网中传播，用户私网VLAN ID在公网中被屏蔽，从而大大地节省了服务提供商紧缺的VLAN ID资源，如下图所示。



在QinQ模式下，PE上用于用户接入的端口被称作用户端口。在用户端口上使能QinQ功能，并为每个用户分配一个SP-ID，此处为3，不同的PE上应该为同一网络用户分配相同的SP-ID。当报文从CE1到达PE1时，带有用户内部网络的VLAN tag 200-300，由于使能了QinQ功能，PE上的用户端口将再次为报文加上另外一层VLAN tag，其ID就是分配给该用户的SP-ID。此后该报文在服务提供商网络中传播时仅在VLAN 3中进行且全程带有两层VLAN tag（内层为进入PE1时的tag，外层为SP-ID），但用户网络的VLAN信息对运营商网络来说是透明的。当报文到达PE2，从PE2上的客户端口转发给CE2之前，外层VLAN tag被剥去，CE2收到的报文内容与CE1发送的报文完全相同。PE1到PE2之间的运营商网络对于用户来说，其作用就是提供了一条可靠的二层链路。

可见，使用QinQ组建VPN具有如下特点：1 无需信令来维持隧道的建立，通过简单的静态配置即可实现，免去了繁杂的配置，维护工作。2运营商只需为每个用户分配一个SP-ID，提升了可以同时支持的用户数目；而用户也具有选择和管理VLAN ID资源的最大自由度（从1-4096中任意选择）。3 在运营商网络的内部，P设备无需支持QinQ功能，即传统的三层交换机完全可以满足需求，极大地保护了运营商的投资。4用户网络具有较高的独立性，在服务提供商升级网络时，用户网络不必更改原有的配置。因此，无论是对于运营商还是用户来说，采用QinQ方式组建VPN都是一种低成本，简便易行，易于管理的理想方式。

由于在用户接入端口使能了QinQ，导致VPN用户的报文在网络上传播时带有两层VLAN tag，此时三层交换机的三层交换功能对于这种特殊的报文失效，因为交换机无法正确地获取报文内携带的IP地址等信息。但我们不必为此担心，因为VPN报文只在SP-ID对应的VLAN内作二层转发，根本无需使用三层信息进行转发。

在使能QinQ的用户接入端口，仍然可以使用acl规则对报文进行流分类，流限速，重定向等qos/acl操作，这无疑有利于运营商面向不同用户提供不同层次的差别服务。对于用户来说，选择适合自己需求的服务能够节省开支；而运营商也可以借此吸引更广泛的用户对象。

6.2 QinQ 配置

在做QinQ配置之前，需要注意以下几点：

管理员先要了解网络中QinQ的实际应用以及交换机在网络中的位置，根据实际网络的需求做QinQ配置。

QinQ配置主要采用静态配置，将交换机的某个端口配置成QinQ customer端口模式时，从用户侧网络进入该端口的带内部tag的包将被打上外部标签发送，而这个外部标签的vlan值是端口的PVID值。

目前提供的SP VLAN的EtherType有0x8100和0x9100两种。

QinQ端口配置包括customer端口（access端口），service provider端口（uplink端口）。QinQ端口的配置在Interface配置模式下输入，显示命令在CLI全局模式下输入。

下面的命令用于配置customer端口，当不输入tpid时，tpid默认为0x8100：

switchport link-type dot1q-in-q customer [tpid]

例如端口1/2配置成customer端口, tpid为0x8100：

Switch(config-ge1/2)# switchport link-type dot1q-in-q customer 0x8100

下面的命令用于配置service provider端口，当不输入tpid时，tpid默认为0x8100：

switchport link-type dot1q-in-q service -provider [tpid]

例如端口1/2配置成service provider端口, tpid为0x9100：

Switch(config-ge1/2)# switchport link-type dot1q-in-q service -provider 0x9100

下面的命令用于清除端口的QinQ配置：

no switchport link-type dot1q-in-q

例如端口1/2，清除端口的QinQ配置：

Switch(config-ge1/2)# no switchport link-type dot1q-in-q

下面的命令用于显示端口的QinQ配置：

show dot1q-in-q

在CLI全局模式下显示端口的QinQ配置：

Switch# show dot1q-in-q

6.3 QinQ 配置示例

6.3.1 配置

在交换机上作如下配置：

设置端口1/2为QinQ Customer端口，tpid为0x8100，端口的PVID值为3（即交换机将对进入该端口的包打上外部vlan值 3），

设置端口2/2为QinQ Customer端口，tpid为0x8100，端口的PVID值为10（即交换机将对进入该端口的包打上外部vlan值 10），

设置端口2/12为QinQ Service Provider端口，tpid为0x8100。

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 3
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
Switch(config)# interface ge1/2
Switch(config-ge1/2)# switchport mode access
Switch(config-ge1/2)# switchport access vlan 3
Switch(config-ge1/2)# switchport link-type dot1q-in-q customer
Switch(config-ge1/2)# interface ge2/2
Switch(config-ge2/2)# switchport mode access
Switch(config-ge2/2)# switchport access vlan 10
Switch(config-ge2/2)# switchport link-type dot1q-in-q customer
Switch(config-ge2/2)# interface ge2/12
Switch(config-ge2/12)# switchport mode trunk
Switch(config-ge2/12)# switchport trunk allowed vlan all
Switch(config-ge2/12)# switchport link-type dot1q-in-q service-provider
```

第7章 配置MSTP

本章对MSTP及其配置进行描述，主要包括以下内容：

- MSTP介绍
- MSTP配置
- MSTP配置示例

7.1 MSTP 介绍

联想天工iSpirit 8806交换机支持IEEE802.1d,IEEE802.1w，IEEE802.1s标准的STP协议。

7.1.1 概述

MSTP,使用RSTP快速收敛，使多个VLAN聚合到一个生成树实例，每个实例有个一个独立于其他生成树实例的生成树拓扑。这个架构为数据流提供多个转发路径，能够负载均衡，并且减少被要求支持大量VLAN的生成树实例。

7.1.2 多生成树域

对于参与多生成树（MST）计算的实例，必须一致地配置交换机相同的MST配置信息。有相同MST配置的相连的交换机集合构成MST域。

MST 配置决定每一个交换机所属的域。配置包括域名，修订版本号，和 MST 实例和 VLAN 指派映射；这些信息在 MST 配置中会生成一个唯一的摘要（Digest)。同一个域中的摘要是相同的，也必须是相同的，可以通过 show spanning-tree mst config 命令查看这些信息。

一个域可以有一个或多个有相同 MST 配置的成员；每一个成员必须有处理 RSTP BPDU 的能力。在一个网络中没有限制 MST 域的数量，但是每个域最多支持 16 个实例。你一次只能分配一个 VLAN 到一个生成树实例中。

7.1.3 IST, CIST, 和 CST

内部生成树（IST)，运行在 MST 域内的生成树。

在每一个 MST 域，MSTP 维护多个生成实例。实例 0 是一个域的一个特殊的实例，被称之为 IST。所有其他 MST 实例是数字 1 到 15。

这个 IST 仅仅是一个接收和发送 BPDU 的生成树实例 ;所有其他生成树实例信息被压缩

在 MSTI BPDU 中。因为 MSTI BPDU 携带所有实例的信息，需要被一个支持多生成树实例的交换机处理 BPDU 的数量意味着要简化。

所有在相同域的 MST 实例共享相同的协议 timer，但是每个 MST 实例有它自己的拓扑参数，例如一个根交换机 ID，根路径花消等等。缺省情况，所有的 VLAN 被分配到 IST。

公用的和内部的生成树（CIST），是每一个 MST 域里的所有 IST，和（连接 MST 域和单个生成树的）公用生成树的集合。

在一个域内计算的生成树看起来像是包含所有交换机域的 CST 的一个子树。CIST 被支持 802.1W 和 802.1D 协议的交换机之间的生成树计算运行的结果形成的。在 MST 域的 CIST 和在域外的 CST 相同。

公共生成树（CST），运行在 MST 域间的生成树。

7.1.4 域内操作

IST 连接一个域内所有 MSTP 交换机。当 IST 收敛时，IST 的根成为 IST master，它是域内最低 bridge ID 和到 CST 根的路径开销的交换机。如果在网络中只有一个域，IST master 也是 CST 根。如果 CST 根在域外，在域的边界（boundary）的一个 MSTP 交换机被选为 IST master。

当一个 MSTP 交换机初始化时，它发送 BPDU 要求它自己作为 CST 根和 IST master，到 CST 根和 IST master 的路径花销设置为 0。交换机也初始化所有的 MST 实例并且要求成为他们的根。如果交换机收到的 MST 根信息比当前端口存储的信息优先（低 bridge ID，低路径花消等等），它放弃它的成为 IST master 的要求。

在初始化中，一个域可能有许多亚域，每一个带有它自己的 IST master。当交换机收到一个更优先的 IST 信息时，它离开它旧的亚域加入到新的可能包含真是 IST master 的亚域。因此所有的亚域都收缩，包含真正的 IST master 的亚域除外。

为了正确的操作，所有的 MST 域内的交换机必须承认相同的 IST master。所以，任意两个域内的交换机同步他们的一个 MST 实例的端口的角色,只是如果它们收敛到一个公用 IST master。

7.1.5 域间操作

如果有多个域或早期 802.1D 交换机在网络中，MSTP 建立和维护 CST，它包含所有网

络中的 MST 域和所有早期 STP 交换机。MST 实例联合在域边界（boundary）的 IST 成为 CST.

IST 连接所有 MSTP 域内的交换机并且看起来像 CST（包围所有交换机域）的一个子树，子树的根成为 IST master。MST 域看起来像一个虚拟的交换机邻接到 STP 交换机和 MST 域。

只不过 CST 实例发送和接收 BPDU，和 MST 实例增加它们的生成树信息到 BPDU 相互影响邻居交换机和计算最后的生成树拓扑。因为这个，涉及到 BPDU 传送 （比如：hello time, forward time, max-age,和 max-hops）的生成树参数被配置仅仅在 CST 实例但是不影响所有 MST 实例。涉及到生成树拓扑的参数（比如：switch priority, port VLAN cost , port VLAN priority）可以被配置在 CST 实例和 MST 实例。

MSTP 交换机使用版本 3 的 RSTP BPDU 或 802.1D 的 BPDU 和 802.1D 的交换机通信。MSTP 交换机使用 MSTP BPDU 和 MSTP 交换机通信。

7.1.6 跳的计数

在配置计算生成树拓扑的 BPDU 中 IST 和 MST 实例不使用 message-age 和 maximum-age 信息。替代为，使用到根的路径花消和相当于 IP TTL 的 hop-count 机制。

你可以配置那个域的最大跳数并应用到那个域 IST 和所有的 MST 实例。跳数计算实现和 message-age 结果相同 (在引发一个重新配置后决定)。实例根交换机总是发送一个 cost 为 0, hop-count 为最大值的 BPDU（or-M-record）。当一个交换机收到 BPDU 时，它把剩余的跳数减 1， 并且在它产生的 BPDU 里面传播这个剩余的跳数。当计数到达 0，交换机丢弃 BPDU 并且 age 这个端口的信息。

在一个域里面，在 RSTP BPDU 部分里面的 Message-age 和 maximum-age 信息保留一致，相同的值被在边界（boundary）的域的指定端口传播。

7.1.7 边界端口

边界端口（boundary）是一个连接 MST 域到一个单独运行 RSTP 的生成树域，或者一个单独 801.1D 的生成树域，或者其他不同配置的 MST 域。一个边界端口也连接到一个 LAN，这个 LAN 的指定交换机要么是一个单独生成树交换机要么是一个带有不同的 MST 域配置的交换机。

在边界端口，MST 端口角色不重要，它们的状态被强制和 IST 端口状态相同（当 IST 端口是 forwarding 时，在边界的 MST 端口是 forwarding）。一个在边界的 IST 端口可以有除备份端口以外的任何角色。

在一个共享边界连接，MST 端口在转换到 learning 状态前，在 blocking 状态等待 forward-delay time 到期。MST 端口在转换到 forwarding 前，等待又一个 forward-delay time 到期。

如果边界端口是一个点到点连接并且是 IST 根端口，IST 端口一转换到 forwarding 状态 MST 端口就转换到 forwarding 状态。

如果一个边界端口在实例中转换到 forwarding 状态，它在所有的实例中都是 forwarding，一个拓扑改变是触发的。如果一个带有 IST 根或指定端口角色的边界端口接收到一个拓扑改变通告，MSTP 交换机在活跃的那个端口上的 IST 实例和所有 MST 实例触发一个拓扑改变。

7.1.8 MSTP 和 802.1d STP 的互用性

一个运行 MSTP 的交换机支持一个内置的协议迁移机制，这个机制使他能够和 802.1D 协调使用。如果交换机从一个端口收到一个 802.1D 配置的 BPDU，它就在那个端口发送 802.1D BPDU。当一个域的边界端口收到一个 802.1D BPDU 一个不同域的 MSTP BPDU 或 RSTP BPDU 时，MSTP 交换机可以侦察到。

然而，如果交换机不再接收 802.1D BPDU 它不会自动恢复到 MSTP 模式，因为它不能决定对方的交换机是否已经从连接删除，除非对方的交换机是指定交换机。同样，当连接到这个交换机的交换机已经加入到这个域时，交换机可能继续分配一个边界端口角色到一个端口。重新启动协议的迁移处理（强制和邻居交换机协商）。

如果所有在连接的对方的交换机是 RSTP 交换机，它们可以处理 MSTP BPDU 和处理 RSTP BPDU。因此，MSTP 交换机在边界端口或者发送一个版本 0 配置和 TCN BPDU 或版本 3MSTP BPDU。一个连接到 LAN 的边界端口，他的指定交换机要么是一个单独生成树交换机或是一个不同 MST 配置的交换机。

7.1.9 端口角色

MSTP 采用 RSTP 的快速收敛算法。下面结合 RSTP 简单介绍 MSTP 端口角色和快速收敛。

RSTP 提供指定端口角色和决定活动拓扑的快速收敛。RSTP 基于 IEEE802.1D STP 之上，选择高优先级交换机作为根交换机。当 RSTP 指定一个端口角色到一个端口时：

Root port － 当交换机转发包到根交换机时提供最优路径花消。

Designated port － 连接指定交换机。当转发从 LAN 到根交换机数据包产生最低的路径花消。指定交换机通过它连接到 LAN 的端口叫指定端口。

Alternate port－ 提供一个当前根端口的到根交换机的替换路径。

Backup port－扮演一个指定端口到生成树叶子的路径的备份。一个 Backup 端口存在仅仅当两个端口一起连接在一个点到点的环路或当一个交换机有两个或多个连接到一个共享 LAN 段。

Disable port－在生成树操作中没有端口角色。

Master port － 位于域根或到总根的最短路径上，它是连接域到总根的端口。

根端口或指定端口角色包含在活动拓扑。替换端口或备份端口角色不包含于活动拓扑。

在一个稳定拓扑和固定端口角色的整个网络，RSTP 确保每一个根端口和指定端口立即迁移到 forwarding 状态当所有的替换端口和备份端口总是在 discarding 状态时。端口状态控制 forwarding 和 learning 处理。

快速收敛

在下列情况下 RSTP 提供快速恢复：交换机故障，端口故障或 LAN 故障，它为边缘端口，新的根端口和连接到一个点到点的连接提供快速恢复：

Edge ports － 如果你配置一个端口作为边缘端口，边缘端口立即迁移为 forwarding 状态。你可以打开它为边界端口仅仅当这个端口连接到一个单独的终端或者确定不需要计算生成树的设备上。

Root ports － 如果 RSTP 选择一个新的根端口。它阻塞一个旧的根端口并且立即迁移新根端口到 forwarding 状态。

Point-to-point links － 如果你连接一个端口到其它端口通过一个点到点连接并且本地端口成为一个指定端口，它和其它端口经过 proposal-agreement 握手协商一个快速迁移确定一个快速收敛无回环（loop-free）拓扑。

拓扑改变

这部分描述 RSTP 和 802.1D 在处理 spanning-tree 拓扑改变的不同。

Detection － 不像802.1D在blocking和forwarding状态之间的任意迁移都会引起拓扑改变，仅仅从blocking迁移到forwarding状态导致RSTP拓扑改变（只是为了增加连通性被考虑拓扑改变）。状态改变在一个边缘的端口（edge port）不会引起拓扑改变。当一个RSTP

交换机侦查到一个拓扑修改，它泛洪它学习到信息到所有的非边缘端口（nonedge ports）除了接收TC信息的端口外。

Notification － 不像802.1D，使用TCN BPDU，RSTP不使用它。然而，为了和802.1D的互用性，RSTP交换机处理并产生TCP BPDU。

Acknowledgement － 当一个RSTP交换机在指定端口接收到一个来自802.1D交换机的TCN信息，它回应一个带有802.1D BPDU 并且设置TCA标志位。然而，如果TC-while timer(与802.1D的topology-change timer相同)是活动的，在根端口连接到802.1D交换机并收到一个带有TCA的配置BPDU，TC-while timer重起（reset）。这个行为只是被要求支持802.1D交换机。RSTP BPDU从来都没有TCA标志位。

Propagation － 当RSTP交换机通过一个指定端口或根端口从其它交换机接收到一个TC信息，它传播到所有非边缘端口，指定端口和根端口（除接收端口以外的）。交换机所有这样的端口启动TC-while timer并且泛洪他们学习的信息。

Protocol migration － 为了向后兼容802.1D交换机，RSTP基于每一个端口选择性发送802.1D配置BPDU和TCN BPDU。

当一个已经初始化，migrate-delay timer启动（指定最小值在RSTP BPDU被发送期间），RSTP BPDU被发送。当这个timer 是活动的，交换机处理所有的从端口接收的BPDU并且忽略协议类型。

在端口的migration-delay timer已经中止以后，如果交换机收到一个802.1D BPDU，它假设它连接到一个802.1D交换机并且启动使用802.1D协议BPDU。然而，如果RSTP交换机正在一个端口使用802.1D BPDU，在timer中止后接收到一个RSTP BPDU，那个端口它重新启动timer并且开始使用RSTP BPDU。

7.1.10 802.1D 生成树简介

生成树协议基于以下几点：

1）有一个唯一的组地址（01-80-C2-00-00-00）标识一个特定 LAN 上的所有的交换机。这个组地址能被所有的交换机识别；

2）每个交换机有一个唯一的标识（Brideg Identifier）；

3）每个交换机的端口有一个唯一的端口标识（Port Identifier）。对生成树的配置进行管理还需要：对每个交换机调协一个相对的优先级；对每个交换机的每个端口调协一个相对的优先级；对每个端口调协一个路径花费。

具有最高优先级的交换机被称为根（root）交换机。每个交换机端口都有一个根路径花

费，根路径花费是该交换机到根交换机所经过的各个网段的路径花费的总和。一个交换机中根路径花费的值为最低的端口称为根端口，若有多个端口具有相同的根路径花费，则具有最高优先级的端口为根端口。

在每个 LAN 中都有一个交换机被称为指定（designated）交换机，它属于该 LAN 中根路径花费最少的交换机。把 LAN 和指定交换机连接起来的端口就是 LAN 的指定端口（designated port）。如果指定交换机中有两个以上的端口连在这个 LAN 上，则具有最高优先级的端口被选为指定端口。

形成一个生成树所必需决定的要素：

1）决定根交换机

a、最开始所有的交换机都认为自己是根交换机；

b、交换机向与之相连的 LAN 广播发送配置 BPDU，其 root_id 与 bridge_id 的值相同；

c、当交换机收到另一个交换机发来的配置 BPDU 后，若发现收到的配置 BPDU 中 root_id 字段的值大于该交换机中 root_id 参数的值，则丢弃该帧，否则更新该交换机的 root_id、根路径花费 root_path_cost 等参数的值，该交换机将以新值继续广播发送配置 BPDU。

2）决定根端口

一个交换机中根路径花费的值为最低的端口称为根端口。

若有多个端口具有相同的最低根路径花费，则具有最高优先级的端口为根端口。若有两个或多个端口具有相同的最低根路径花费和最高优先级，则端口号最小的端口为默认的根端口。

3）认定 LAN 的指定交换机

a、开始时，所有的交换机都认为自己是 LAN 的指定交换机。

b、当交换机接收到具有更低根路径花费的（同一个 LAN 中）其他交换机发来的 BPDU，该交换机就不再宣称自己是指定交换机。如果在一个 LAN 中，有两个或多个交换机具有同样的根路径花费，具有最高优先级的交换机被选为指定交换机。

c、如果指定交换机在某个时刻收一了 LAN 上其他交换机因竞争指定交换机而发来的配置 BPDU，该指定交换机将发送一个回应的配置 BPDU，以重新确定指定交换机。

4）决定指定端口

LAN 的指定交换机中与该 LAN 相连的端口为指定端口。若指定交换机有两个或多个端口与该 LAN 相连，那么具有最低标识的端口为指定端口。

除了根端口和指定端口外，其他端口都将置为阻塞状态。这样，在决定了根交换机、交

换机的根端口、以及每个 LAN 的指定交换机和指定端口后，一个生成树的拓扑结构也就决定了。

7.2 MSTP 配置

7.2.1 缺省配置

命令参数	缺省值
spanning-tree mst enable(启动 mstp)	关闭
Spanning-tree mst priority(交换机 cist 优先级)	32768
spanning-tree mst hello-time(交换机 cist hello-time)	2 秒
spanning-tree mst forward-time(交换机 cist forward-time)	15 秒
spanning-tree mst max-age(交换机 cist max-age)	20 秒
spanning-tree mst max-hops(交换机 cist max-hops)	20 秒
instance 1 priority (实例优先级)	32768
spanning-tree mst instance 1 priority(端口实例 priority)	128
spanning-tree mst instance 1 path-cost(端口实例 path-cost)	20000000
spanning-tree mst priority （端口 cist priority）	128
spanning-tree mst path-cost（端口 cist path-cost）	20000000

7.2.2 一般配置

启动MSTP

系统在启动时缺省配置MSTP是关闭的。

启动MSTP的配置过程是：

```
Switch#configure terminal
Switch(config)#spanning-tree mst enable
```

关闭MSTP的命令是：

Switch#configure terminal

Switch(config)#no spanning-tree mst

配置max-age

配置max-age是对所有的实例的配置，max-age是交换机在触发一个重新配置前，等待接收生成树配置信息的秒数。

缺省配置是20秒，配置范围是6到40秒。

配置过程：

Switch#configure terminal

Switch(config)#spanning-tree mst max-age <seconds>

配置max-hops

max-hops是在一个域中在BPDU被丢弃前指定的跳数。

缺省值是20，配置范围是1到40。

配置过程：

Switch#configure terminal

Switch(config)#spanning-tree mst max-hops <hop-count>

配置forward-time

配置forward-time是对所有的实例。forward-time是端口从discarding到learning以及learning到forwarding等待的秒数。

缺省配置是15秒，配置范围是4到30秒。根据生成数协议forward-time 必须满足下列条件：2*(forward-time – 1) >= max-age。

配置过程：

Switch#configure terminal

Switch(config)#spanning-tree mst forward-time <seconds>

配置hello-time

配置hello-time是对所有实例的配置。hello-time是根交换机产生配置信息的间隔时间。

缺省配置时间是2秒，配置范围是1到10秒。根据生成数协议hello-time 必须满足下列条件：2*(hello-time + 1) =< max-age。

配置过程：

Switch#configure terminal

Switch(config)# spanning-tree mst hello-time <seconds>

配置CIST bridge的优先级（priority）

缺省配置32768、配置范围<0-61440>；CIST优先级的值只能是4096的倍数。

配置过程：

Switch#configure terminal

Switch(config)#spanning-tree mst priority <priority>

配置和CISCO兼容

联想天工网络交换机采用基于802.1s的MSTP协议，每个MSTI消息的长度是16个字节；而CISCO交换机的BPDU每个MSTI消息的长度是26个字节。为了和CISCO交换机互用，配置联想天工网络的交换机时要启动和CISCO兼容的开关。

在启动和CISCO兼容配置的情况下，在判断是否为相同的域时，只要域名和修订版本号相同就认为是相同的域。

缺省系统不启动这个功能。

打开和CISCO兼容：

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability enable

关闭和CISCO兼容：

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability disable

复位协议检查任务

为了和802.1D STP协议的兼容，系统可以自动侦察对方系统运行的协议。根据对方运行的协议来决定这个端口运行的协议。

有些情况下要复位协议。例如系统经过协商一个端口运行STP协议，一段时间后对方的运行STP协议的设备已替换为一台主机。这时我需要配置这个端口为fast port，但是该端口已经运行了stp协议，而且协议协商的任务已经停止；这时需要复位这个协议协商的任务让它重新协商它和主机之间的协议。

复位整个设备的协议侦察任务：

Switch#clear spanning-tree detected protocols

复位某个端口的协议侦察任务：

Switch#clear spanning-tree detected protocols interface <if-name>

7.2.3 域配置

两个或者多个设备在相同的域，他们必须有相同的 VLAN 实例映射关系，相同的修改版本号和相同的域名。

一个域有一个或多个有相同 MST 配置的成员，每个成员都可以处理 RSTP BPDUS 能力。在一个网络中不限制成员数量，但是每个域最多能够支持 16 个实例。

关于实例的配置在'实例配置'里面说明，这里只介绍域名配置和修订版本号配置。

配置域名：

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#region <region-name>
```

配置修订版本号：

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# revision <revision-num>
```

7.2.4 实例配置

系统支持 16 个实例，实例 ID 号的范围是 0-15。一个 VLAN 一次只能分配到一个生成树实例。

缺省情况只存在一个实例0，所有的VLAN都属于这个实例。

配置一个实例的过程：

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance <instance-id> vlan <vlan-id>
```

配置MSTI bridge的优先级（priority）

缺省配置 32768、配置范围<0-61440>；MSTI 优先级的值只能是 4096 的倍数。

配置过程：

```
Switch#configure terminal
```

Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance <instance-id> priority <priority>

7.2.5 端口配置

下面介绍MSTP相关的端口配置信息。这里只介绍简单配置部分，port fast和root guard在后面单独介绍。

配置一个端口加入到一个实例的过程：
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id>

配置CIST 端口的优先级（priority）
缺省配置128，配置范围是<0-240>,CIST端口的优先级的值只能是16的倍数。
配置过程：
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst priority <priority>

配置MSTI端口的优先级（priority）
缺省配置128，配置范围是<0-240>,MSTI端口的优先级的值只能是16的倍数。
配置过程：
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id> priority <priority>

配置CIST端口的路径花消（path-cost）
缺省配置 20000000，配置范围是 1-200000000。下面是带宽和路径花消映射表：

带宽(bps)	路径花消
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000

100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

配置过程

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst path <path-cost>

配置MSTI端口的路径花消（path-cost）

缺省配置20000000，配置范围是1-200000000。带宽和路径花消和上面的表一样。

配置过程

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> path-cost <path-cost>

配置发送协议包的版本号

缺省配置发送MSTP协议包，配置范围是0-3,映射关系是0-stp,2-rstp,3-mstp。

配置过程：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)# spanning-tree mst force-version <version-id>

配置连接类型

如果一个端口通过点到点的方式连接到其它的端口，并且本地端口成为一个designated port（指定端口）,RSTP通过proposal-agreement(提议-协定)过程协商一个快速迁移它所连接的端口成为根端口来确定一个无环的拓扑。

下面简单介绍proposal-agreement的协商过程。

当交换机在它的一个端口收到一个提议信息并且那个端口被选择为新的根端口，RSTP强迫所有其它端口同步新根端口信息。

如果其它所有的端口被从根端口接收的更优的（superior）根信息同步，那么交换机被同步。

当RSTP强制它同步新的根信息时，如果一个指定端口是在forwarding状态，而且没有被配置为一个边缘端口，它迁移到blocking状态。通常，当RSTP强制一个端口同步新的根消息并且端口不能满足上面的条件时，端口状态设置为blocking。

当确保所有的端口被同步，交换机发送一个agreement信息到根端口相应的指定端口。当交换机连接到一个点到点连接在agreement他们的端口角色，RSTP立即迁移端口状态为forwarding。

如果是共享连接，则要经过802.1D的计算过程来确定端口的状态。

缺省情况端口连接类型是点到点的连接。

配置端口的连接类型是点到点的连接：

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst link-type point-to-point
```

配置端口的连接类型是共享连接：

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config-ge2/1)#spanning-tree mst link-type shared
```

7.2.6 PORTFAST 相关配置

1) Port Fast

Port Fast 立即转移一个 access 或 trunk 端口从 blocking 状态到 forwarding 状态，绕过 listening 和 learning 状态。你可以用 Port Fast 在连接一个单独工作站和服务器，可以允许这些设备立即连接到网络，不需要等待 spanning tree 收敛。

配置一个端口为 fast port：

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst portfast
```

2) BPDU Filtering

BPDU filtering可以基于交换机全局打开或者基于每个端口打开，但是他们的特点是不

一样的。

在全局层，你可以用spanning-tree mst portfast bpdu-filter命令启动在portfast bpdu-filter default状态的端口的BPDU filtering功能。

在端口层，你可以用 spanning-tree mst portfast bpdu-filter enable 在任意端口打开BPDU filter。

这个功能防止 port fast 端口接收或发送 BPDU。

配置 BPDU Filtering

在全局配置模式下：

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-filter

在接口配置模式下：

Switch#configure terminal

Switch#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-filter enable

3) BPDU Guard

BPDU 保护特性可以在交换机全局打开或是基于每个端口被打开，但是他们的特点是不一样的。

在全局层,你可以用 spanning-tree mst portfast bpdu-guard 打开在 portfast bpdu-gurad default 状态的端口的 BPDU guard 功能。

在端口层，你可以在任何端口打开 BPDU guard。

当配置了 BPDU gurad 的端口收到 BPDU 时，spanning tree 会 shutdown 这个的端口。在一个有效的配置，Port Fast-enabled 的端口不接收 BPDU。在一个 Port Fast-enabled 的端口接收到一个 BPDU 表示一个无效的配置，例如是一个未授权设备的连接，BPDU guard 进入到一个 error-disabled 状态。

error-disabled 是当启动 BPDU gurad 的端口收到 BPDU 时,如果系统配置 error-disable 机制时会启动 error-disable timer。error-disable 会在系统配置的超时时间后重新启动这个端口。

在全局配置模式下：

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-guard

在接口配置模式下：

Switch#configure terminal

Switch#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-guard enable

error-disable 的配置

启动 error-disable 机制

Switch#configure terminal

Switch#spanning-tree mst errdisable-timeout enable

配置 error-disable 超时时间

Switch#configure terminal

Switch# spanning-tree mst errdisable-timeout interval <seconds>

7.2.7 Root Guard 相关配置

一个 SP 的二层网络可以包含许多连接到不属于他们自己的交换机。在这样一个拓扑，生成树可以重新配置它自己并且选择一个客户交换机作为根交换机。你可以通过配置 root guard 在 SP 交换机的连接到在客户网络的交换机的端口避免这种情况。如果生成树计算导致在客户网络的端口被选为 root port，root guard 就配置端口为 root-inconsistent(blocked)状态防止客户交换机成为根交换机或存在到根的路径。

如果一个 SP 网络外面的交换机成为根交换机，端口是 blocked（root-inconsistent stat）并且生成树选择一个新的根交换机。客户的交换机不会成为根交换机并且不存在到根的路径。

如果交换机在 MST 模式操作，root guard 强制端口成为指定端口。如果一个边界端口因为 root guard 在 IST 实例是 blocked 状态，这端口在所有的 MST 实例是 block 的。一个边界端口是连接到一个 LAN 的端口，指定交换机要么是一个 802.1D 交换机或一个不同 MST 域配置的交换机。

在一个端口被打开 Root guard 应用到所有的这个端口所属的 VLAN。VLAN 可以被聚合并映射到一个 MST 实例。

配置过程

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst guard root

7.3 MSTP 配置示例

(1)配置

三台交换机连接成一个环状，需要打开每一台交换机的生成树协议，避免环路的发生。分别在每一台交换机上执行配置。

交换机1的配置：

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable

交换机2的配置：

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable

交换机3的配置：

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable



(2)排错：

查看哪一个交换机被选为根网桥：

执行show spanning-tree mst，观察CISTRoot的值为三台交换中MAC地址最小的一个，即根选举结果正确。

Switch#show spanning-tree mst

查看生成树中交换机的端口状态：

执行show spanning-tree mst interface ge1/1这条指令，观察PORT ge1/1在实例0中的State 值

Switch#show spanning-tree mst interface ge1/1

第8章 配置EAPS

8.1 EAPS 简介

EAPS是Ethernet Automatic Protecting Switching的简称。EAPS利用标准的Ethernet和VLAN技术提供环路拓扑和环路恢复机制。在环中出现故障时EAPS有能力在1秒内恢复数据通信。EAPS运行不受节点个数的限制，环的恢复时间也不受节点数的限制。EAPS不依赖其它的设备，也就是说EAPS环中可以有不支持EAPS协议的设备。

8.2 EAPS 基本概念

下面介绍EAPS涉及到的一些基本概念：

1、EAPS Domain， 在一个网络中，一个EAPS Domain是在一个单独的环中运行的。它是组成一个单独环路的一系列的节点设备，一个EAPS Domain包含一个Master Node和一个或多个Transit Node。

2、Master Node，一个运行EAPS的交换机或称之为EAPS节点设备，一个EAPS

Domain有且仅有一个Master Node。

3、Transit Node，一个运行EAPS的交换机或称之为EAPS节点设备，在一个EAPS Domain中除Master Node外的其它节点。

4、Primary Port，一个EAPS Domain中连接EAPS节点设备的端口。一个节点设备在一个EAPS Domain中有且仅有一个Primary Port连接到这个环。

5、Secondary Port，一个EAPS Domain中连接EAPS节点设备的端口。一个节点设备在一个EAPS Domain中有且仅有一个Secondary Port连接到这个环。

6、Control VLAN，控制VLAN，负责EAPS Domain协议包传输的VLAN，一个EAPS Domain中有且仅有一个Control VLAN。

7、Protected VLAN，被保护VLAN，在EAPS Domain中传输业务数据的VLAN，一个EAPS Domain中必须有一个Protected VLAN，也可以多于一个Protected VLAN。

8.3 EAPS 协议介绍

一个EAPS Domain运行在一个EAPS环上。一个EAPS Domain中包含一个Master Node与一个或多个Transit Node；每个EAPS节点包含一个相同的Control VLAN和多个Protected VLAN；每个EAPS节点在一个EAPS Domain中包含一个Primary Port和一个Secondary Port，这两个端口都属于这个环的Control VLAN和所有Protected VLAN。 通过每个EAPS节点设备的Primary Port和Secondary Port连接这个EAPS Domain中的所有节点组成一个EAPS环。

在正常情况下，当EAPS Domain中所有的Primary Port和Secondary Port都LINK UP时，阻塞Master Node的Secondary Port（置Secondary Port的端口状态为Blocking），消除EAPS Domain中的业务数据的环路。当EAPS Domain出现故障时，立即打开Master Node的Secondary 端口（置Secondary Port的状态为Forwarding），允许它转发业务数据，恢复业务数据的正常转发。

Transit Node对Primary Port和Secondary Port处理没有任何区别。

下面介绍EAPS的两种故障检查和环路恢复：

8.3.1 Link-Down 报警

当Transit Node发现自己的Primary Port或Secondary Port端口出现LINK DOWN时，会

立即通过另外一个LINK UP 的端口从Control VLAN发送一个LINK-DOWN协议包给Master Node。

当Master Node收到这个LINK-DOWN协议包时：

Master Node立即由Complete状态进入Failed状态，打开Secondary Port（置Secondary Port的状态为Forwarding），刷新自己的二三层转发表，发送一个RING-DOWN-FLUSH-FDB通知EAPS Domain其它的Transit刷新自己的转发表，重新学习二三层转发表。

当Master Node发现本地的Primary Port发生LINK DOWN时，它的操作和收到LINK-DOWN协议包的操作是相同的。

当Master Node发现本地的Secondary Port发生LINK DOWN时，Master Node立即由Complete状态进入Failed状态，刷新自己的二三层转发表，发送RING-DOWN-FLUSH-FDB协议包，通知EAPS Domain其它的Transit刷新自己的转发表，重新学习二三层转发表。

8.3.2 环路检查

Master Node会定期的从Primary Port发送HEALTH协议包。如果环是完整的，Master Node可以在自己的Secondary Port收到这个HEALTH协议包，这时Master Node会重启它的Fail-period定时器，Master Node的状态是Complete。

如果fail-period到期前没有收到自己的HEALTH协议包，Master Node将离开Complete状态，进入Failed状态，打开Secondary Port（置Secondary Port的状态为Forwarding），刷新自己的二三层转发表，发送RING-DsOWN-FLUSH-FDB通知EAPS Domain其它的Transit刷新自己的转发表，重新学习二三层转发表。

8.3.3 环的恢复

Master Node不管环是Complete或者是Failed或其它的情况下都会从它的Primary Port发送HEALTH协议包。当Master Node处于Failed状态的情况下，一旦从它的Secondary Port收到HEALTH协议包，环就会恢复到Complete状态。这时Master Node就会设置Secondary Port的状态为blocking状态，刷新自己的二三层转发表，并发送一个RING-UP-FLUSH-FDB包，通知其它的设备刷新自己的二三层转发表，重新学习二三层转发表。

在Transit Node的端口由LINK DOWN回到LINK UP和Master Node发现环恢复期间，Master Node的Secondary Port可能仍然处于Forwarding状态，这种情况下会造成一个临时环。因此在Transit Node在一个端口是LINK UP状态，另外一个LINK DOWN的端口也变成LINK UP时，Transit Node要进入到一个“前Forwarding状态”（PRE-FORWARDING），

在这个状态下后面LINK UP的端口也会处于Pre-forwarding状态，不能转发业务数据，打断可能出现的数据环路。等到Master Node恢复并发送RING-UP-FLUSH-FDB时，Transit Node收到这个协议包后会把节点状态切换到LINK-UP状态，把Pre-forwarding状态的端口设置为Forwarding状态，恢复业务数据的正常转发。

如果Transit Node收不到RING-UP-FLUSH-FDB协议包，它会在双倍的fail-time的时间后，由Pre-forwarding状态的端口设置为Forwarding状态。

8.3.4 兼容 Extreme 的 EAPS

Extreme公司的产品是最早支持EAPS的厂家，iSpirit8806设备支持的EAPS协议是遵循RFC3619的标准的；而Extreme设备的EAPS协议包和RFC3619的协议包定义有一些区别。联想网络的iSpirit8806设备支持的EAPS协议完全可以和Extreme设备兼容，而且在缺省的情况下兼容开关是打开的。

8.3.5 多 EAPS Domain

iSpirit8806设备可以支持多个EAPS Domain，共支持16个。

8.4 EAPS 配置

EAPS协议的基本配置包含以下几个基本要素：Control VLAN，节点模式（mode），Primary Port，Secondary Port，Protected VLAN，Hello Time和Fail Time。Hello Time和Fail Time有缺省的配置，Hello Time是1秒，Fail Timer是3秒。

8.5 限制条件

1、Primary Port必须属于一个EAPS Domain 的Control VLAN和所有Protected VLAN的TRUNK 模式成员。

2、EAPS 协议不能和MSTP协议同时运行，如果启动了MSTP或配置了MSTP 实例都不能启动EAPS协议。

3、一个VLAN启动了VLLP协议就不能配置为EAPS的Control VLAN或Protected VLAN。

4、EAPS的Control VLAN只能包含Primary Port和Secondary Port，而且只能是VLAN的TRUNK模式。

5、一个VLAN如果被配置为EAPS的Domain的Control VLAN，而且这个Domain已经启动，那么这个VLAN不能被删除，它的端口成员也不能被修改或删除。Control VLAN不能配

置三层接口。

6、Protected VLAN中Primary Port和Secondary Port只能是TRUNK模式。其它成员端口不限制。

7、一个端口只能配置为一个EAPS Domain的Primary Port或者是Secondary Port。

8、同一个VLAN也只能属于一个EAPS Domain的Control VLAN或Protected VLAN。

9、一个EAPS Domain中所有节点的控制VLAN必须是相同的。

8.6 EAPS 命令的简单介绍

要创建一个EAPS Domain，首先要确保VLAN和端口的配置要符合上面的条件。

配置EAPS有一定的顺序要求，先要创建一个EAPS Domain，在启动EAPS Domain前，要按照前面的要求配置其它的参数；否则启动会不成功。如果要把hello time修改成大于当前的fail time的值，要先把fail time修改为更大的数；否则会配置不成功。其它的配置顺序没有特别要求。

在一个EAPS Domain已经启动的情况下，control-vlan，mode，primary-port, secondary-port不能被修改; protected-vlan, fail-timer, hello-time, extreme-interoperability可以被修改。

Primary-port和secondary-port支持LACP端口（也就是TRUNK组）。

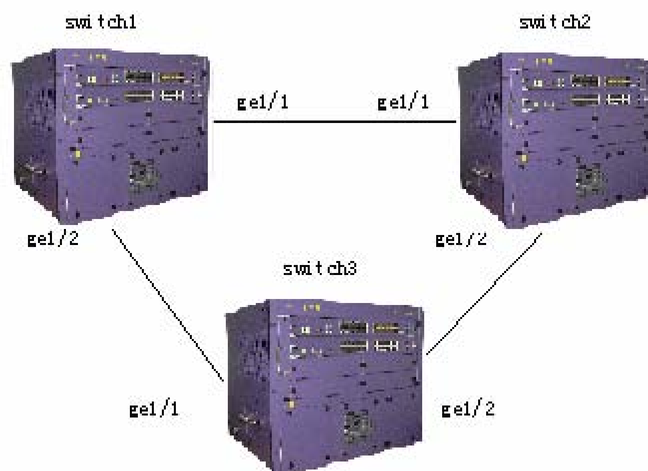
8.6.1 EAPS 配置命令

命令	描述	模式
eaps create <ring-id>	创建一个 EAPS Domain	全局配置模式
eaps control-vlan <ring-id> <vlan-id>	配置一个 EAPS Domain 的控制 VLAN。	全局配置模式
eaps protected-vlan <ring-id> <vlan-id>	增加一个 EAPS Domain 的被保护 VLAN。	全局配置模式
eaps mode <ring-id> <master|transit>	配置一个 EAPS Domain 的运行节点模式。	全局配置模式
eaps primary-port <ring-id> <ifname>	配置一个 EAPS Domain 的 Primary Port。	全局配置模式
eaps secondary-port <ring-id> <ifname>	配置一个 EAPS Domain 的 Secondary Port。	全局配置模式
eaps fail-time <ring-id> <secs>	配置一个 EAPS Domain 的 fail-period timer 超时的时间。缺省是 3 秒。单位是秒。	全局配置模式
eaps hello-time <ring-id> <secs>	配置一个 EAPS Domain 定时发送 HEALTH 包的时间。缺省是 1 秒。单位是秒。Hello-timer 必须	全局配置模式

	小于 fail-time。	
eaps extreme-interoperability <ring-id> <enable|disable>	启动或关闭和 Extreme 设备兼容，缺省是启动兼容。	全局配置模式
eaps enable <ring-id>	启动一个 EAPS Domain	全局配置模式
eaps disable <ring-id>	关闭一个 EAPS Domain	全局配置模式
show eaps	显示系统中启动了了的 EAPS Domain 的信息	普通模式/特权模式
Show eaps <ring-id>	显示一个 EAPSDomain 的详细信息	普通模式/特权模式

8.7 配置示例

有三台iSpirit8806设备switch1，switch2，switch3，要通过EAPS协议保护VLAN 1在流量转发时不会形成环路，同时保证当switch1，switch2，switch3之间有一条链路断开的情况下启用备用链路。根据上面的要求可以把switch1配置为master模式；把switch2和switch3配置为transit模式。增加一个协议包传输的控制VLAN VLAN 2。



switch1的配置：

switch1被配置为EAPS Domain ring 1的master，控制VLAN是VLAN 2，被保护VLAN是VLAN 1，primary-port是ge1/1，secondary-port是ge1/2，其它配置采用缺省值。

Switch#configure terminal

#添加VLAN 2

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

#把ge1/1配置为VLAN 1和VLAN 2的trunk成员。

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#把ge1/2配置为VLAN 1和VLAN 2的trunk成员。

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport mode trunk

Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit

Switch(config)#exit

Switch#show vlan

```
 VLAN   Name        State        Member ports ([u]-Untagged, [t]-Tagged)
 ----   --------    ---------    -------------------------------------------------
 1      vlan1       active       [u]ge0/1 [t]ge0/2 [u]ge0/3 [u]ge0/4 [u]ge0/5
                                 [u]ge0/6 [u]ge0/7 [u]ge0/8 [u]ge0/9 [u]ge0/10
                                 [u]ge10/11   [u]ge0/12   [t]ge1/1   [t]ge1/2   [u]ge1/3
                                 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9
                                 [u]ge1/10  [u]ge1/11  [u]ge1/12  [u]ge1/13  [u]ge1/14
                                 [u]ge1/15  [u]ge1/16  [u]ge1/17  [u]ge1/18  [u]ge1/19
                                 [u]ge1/20 [u]ge1/21 [u]ge1/22 [u]ge1/23 [u]ge1/24
 2      vlan2       active       [t]ge1/1 [t]ge1/2
```

Switch#configure terminal

#创建一个EAPS Domain ring 1

Switch(config)#eaps create 1

#把VLAN 2配置为控制VLAN

Switch(config)#eaps control-vlan 1 2

#把VLAN 1配置为被保护VLAN

Switch(config)#eaps protected-vlan 1 1

#把switch1配置为master节点

Switch(config)#eaps mode 1 master

#把ge1/1配置为primary-port

Switch(config)#eaps primary-port 1 ge1/1

#把ge1/2配置为secondary -port

Switch(config)#eaps secondary-port 1 ge1/2

#启动EAPS Domain ring 1

Switch(config)#eaps enable 1

Switch2的配置

Switch2被配置为EAPS Domain ring 1的transit，控制VLAN是VLAN 2，被保护VLAN是VLAN 1，primary-port是ge1/1，secondary-port是ge1/2，其它配置采用缺省值。

Switch#configure terminal

#添加VLAN 2

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

#把ge1/1配置为VLAN 1和VLAN 2的trunk成员。

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#把ge1/2配置为VLAN 1和VLAN 2的trunk成员。

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport mode trunk

Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit

```
Switch(config)#exit
Switch#show vlan
 VLAN   Name        State       Member ports ([u]-Untagged, [t]-Tagged)
 ----   --------    ---------   ------------------------------------------------
 1      vlan1       active      [u]ge0/1 [t]ge0/2 [u]ge0/3 [u]ge0/4 [u]ge0/5
                                 [u]ge0/6 [u]ge0/7 [u]ge0/8 [u]ge0/9 [u]ge0/10
                                 [u]ge10/11  [u]ge0/12  [t]ge1/1  [t]ge1/2  [u]ge1/3
                                 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9
                                 [u]ge1/10  [u]ge1/11  [u]ge1/12  [u]ge1/13  [u]ge1/14
                                 [u]ge1/15  [u]ge1/16  [u]ge1/17  [u]ge1/18  [u]ge1/19
                                 [u]ge1/20 [u]ge1/21 [u]ge1/22 [u]ge1/23 [u]ge1/24
 2      vlan2       active      [t]ge1/1 [t]ge1/2


Switch#configure terminal

#创建一个EAPS Domain ring 1
Switch(config)#eaps create 1

#把VLAN 2配置为控制VLAN
Switch(config)#eaps control-vlan 1 2

#把VLAN 1配置为被保护VLAN
Switch(config)#eaps protected-vlan 1 1

#把switch配置为transit节点
Switch(config)#eaps mode 1 transit

#把ge1/1配置为primary-port
Switch(config)#eaps primary-port 1 ge1/1

#把ge1/2配置为secondary -port
Switch(config)#eaps secondary-port 1 ge1/2

#启动EAPS Domain ring 1
Switch(config)#eaps enable 1
```

Switch3的配置

Switch3被配置为EAPS Domain ring 1的transit，控制VLAN是VLAN 2，被保护VLAN是VLAN 1，primary-port是ge1/1，secondary-port是ge1/2，其它配置采用缺省值。

```
Switch#configure terminal

#添加VLAN 2
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit

#把ge1/1配置为VLAN 1和VLAN 2的trunk成员。
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#把ge1/2配置为VLAN 1和VLAN 2的trunk成员。
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan
 VLAN   Name      State      Member ports ([u]-Untagged, [t]-Tagged)
 ----   --------  ---------  ------------------------------------------------
 1      vlan1     active     [u]ge0/1 [t]ge0/2 [u]ge0/3 [u]ge0/4 [u]ge0/5
                             [u]ge0/6 [u]ge0/7 [u]ge0/8 [u]ge0/9 [u]ge0/10
                             [u]ge10/11 [u]ge0/12 [t]ge1/1 [t]ge1/2 [u]ge1/3
                             [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9
                             [u]ge1/10 [u]ge1/11 [u]ge1/12 [u]ge1/13 [u]ge1/14
                             [u]ge1/15 [u]ge1/16 [u]ge1/17 [u]ge1/18 [u]ge1/19
                             [u]ge1/20 [u]ge1/21 [u]ge1/22 [u]ge1/23 [u]ge1/24
 2      vlan2     active     [t]ge1/1 [t]ge1/2
```

Switch#configure terminal

#创建一个EAPS Domain ring 1

Switch(config)#eaps create 1

#把VLAN 2配置为控制VLAN

Switch(config)#eaps control-vlan 1 2

#把VLAN 1配置为被保护VLAN

Switch(config)#eaps protected-vlan 1 1

#把switch3配置为transit节点

Switch(config)#eaps mode 1 transit

#把ge1/1配置为primary-port

Switch(config)#eaps primary-port 1 ge1/1

#把ge1/2配置为secondary -port

Switch(config)#eaps secondary-port 1 ge1/2

#启动EAPS Domain ring 1

Switch(config)#eaps enable 1

第9章 配置IGMP SNOOPING

在城域网/Internet中，采用单播方式将相同的数据包发送给网络中的多个而不是全部接收者时，由于需要复制分组给每一个接收端点，随着接收者数量的增多，需要发出的包数也会线性增加，这使得主机、交换路由设备及网络带宽资源总体负担加重，效率受到极大影响。随着多点电视会议、视屏点播、群组通信应用等需求的增长，为提高资源利用率，组播方式日益成为多点通信中普遍采用的传输方式。

iSpirit 8806交换机实现了IGMP SNOOPING功能，为组播应用服务。IGMP SNOOPING监听网络上的IGMP包，实现IP组播MAC地址的动态学习。

本章对IGMP SNOOPING的概念和配置进行描述，主要包括以下内容：

- IGMP SNOOPING 介绍
- IGMP SNOOPING 配置
- IGMP SNOOPING 配置示例

9.1 IGMP SNOOPING 介绍

传统的网络在一个子网内组播数据包当作广播处理，这样容易使网络流量大，造成网络拥塞。当交换机上实现了IGMP SNOOPING后，IGMP SNOOPING可以动态学习IP组播MAC地址，维护IP组播MAC地址的输出端口列表，使组播数据流只往输出端口发送，这样可以减少网络的流量。

本节主要包括以下内容：

- IGMP SNOOPING 处理过程
- 二层动态组播
- 加入一个组
- 离开一个组

9.1.1 IGMP SNOOPING 处理过程

IGMP SNOOPING是一个二层的网络协议，监听经过交换机的IGMP 协议包，根据这些IGMP协议包的接收端口，VLAN ID和组播地址来维护一个组播组，然后转发这些IGMP 协议包。只有加入了组播组的端口才可以接收组播数据流；这样就减少了网络的流量，节省了网络带宽。

组播组包括了组播组地址，成员端口，VLAN ID，Age时间。

IGMP SNOOPING组播组的形成是一个学习的过程。当交换机的某一个端口收到IGMP REPORT包时，IGMP SNOOPING会产生一个新的组播组，接收IGMP REPORT包的端口就被加入这个组播组。在交换机收到一个IGMP QUERY包时，如果这个组播组已经存在交换机中，那么这个收到IGMP QUERY的端口也加入到这个组播组中，否则只是转发IGMP QUERY包。IGMP SNOOPING还支持IGMP V2的Leave机制；如果IGMP SNOOPING配置了fast-leave 为ENABLE，在收到IGMP V2的leave包时它接收端口可以立刻离开组播组；如果配置了fast-leave离开等待时间(fast-leave-timeout)，那么组播组在等待这个时间到期后再离开组播组。

IGMP SNOOPING有两种更新机制。一种是上面介绍的leave机制。大多数情况下IGMP SNOOPING是通过age time来删除过期的组播组的。当组播组加入IGMP SNOOPING时记录了加入的时间，当组播组在交换机中存留的时间超过了一个配置的age time时，交换机会删除这个组播组。

当一个端口收到Leave协议包时，这个端口会立即从它所属的组播组中删除，这种情况可能会影响网络数据流的连续性；因为这端口下面可能连接着一个HUB或没有IGMP SNOOPING功能的网络设备，这个设备下连接了很多的接收组播数据流设备。一个设备发送Leave，可能会影响其他设备也接收不到组播数据流。Fast-leave-timeout机制可以防止这种情况的发生，通过Fast-leave-timeout配置一个离开等待的时间，端口收到leave包后等待Fast-leave-timeout长的时间再从它所属的组播组中删除，可能保障网络组播流的连续性。

9.1.2 二层动态组播

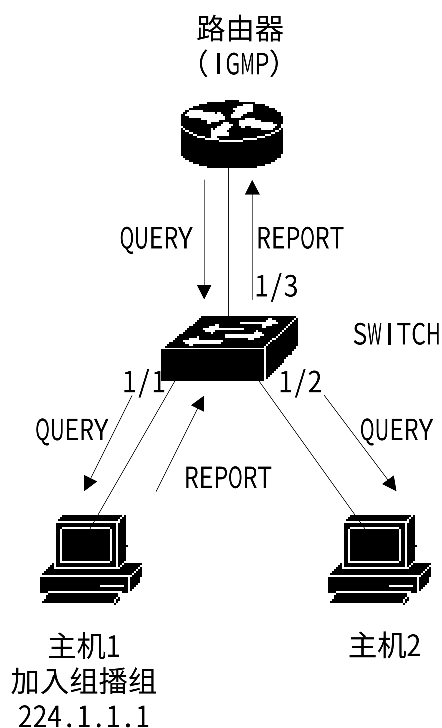
二层硬件组播转发表中的组播MAC地址条目可以通过IGMP SNOOPING动态学习得到。通过IGMP SNOOPING动态学习到的是IP组播MAC地址。

当交换机关闭IGMP SNOOPING时，二层硬件组播转发表处于未注册转发模式，组播MAC地址不能动态学习到，二层硬件组播转发表中没有条目，所有的二层组播数据流当作广播处理。

当网络具备组播环境时，为了有效控制网络的组播流量，交换机可以打开IGMP SNOOPING，此时二层硬件组播转发表处于注册转发模式，交换机可以通过监听网络上的IGMP协议包学习到组播MAC地址，与二层硬件组播转发表中的条目匹配的二层组播流才能够转发。

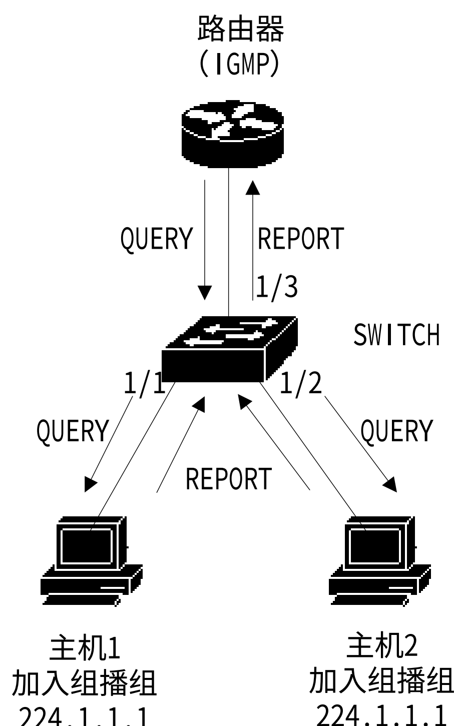
9.1.3 加入一个组

当一个主机想加入一个组播组时，主机会发一个IGMP REPORT包，在此包中指定主机要加入的组播组。当交换机收到一个IGMP QUERY包时，交换机会把该包转发给同一个VLAN的所有其它端口，当端口下的想加入组播组的主机收到IGMP QUERY包后会回送一个IGMP REPORT包。当交换机收到一个IGMP REPORT包后，会建立一个二层组播条目，收到IGMP QUERY包的端口和IGMP REPORT包的端口会加入到该二层组播条目，成为它的输出端口。



如上图所有的设备在一个子网内，假设该子网的VLAN是2。路由器运行IGMPv2协议，定时发送IGMP QUERY包。主机1想加入组播组224.1.1.1。交换机从1/3端口收到IGMP QUERY包后会记录此端口并把该包转发给端口1/1和1/2。主机1收到IGMP QUERY包后回送一个IGMP REPORT包，主机2因为不想加入组播组，不发IGMP REPORT包。交换机从端口1/1收到IGMP REPORT包后会把该包从查询端口1/3转发出去并且创建一个二层组播条目（假定该条目不存在），该二层组播条目包括以下几项：

二层组播地址	VLAN ID	输出端口列表
01:00:5e:01:01:01	2	1/1，1/3



如上图的条件与图1一样，主机1已经加入了组播组224.1.1.1，现在主机2想加入组播组224.1.1.1。当主机2收到IGMP QUERY包后回送一个IGMP REPORT包，交换机从端口1/2收到IGMP REPORT后会把该包从查询端口1/3转发出去并且会包端口1/2加入到二层组播条目中，该二层组播条目变为：

二层组播地址	VLAN ID	输出端口列表
01:00:5e:01:01:01	2	1/1，1/2，1/3

9.1.4 离开一个组

为了能够组成一个稳定的组播环境，运行IGMP的设备（如路由器）会每隔一定的时间发送一个IGMP QUERY包给所有的主机。已经加入组播组或想加入组播组的主机收到该IGMP QUERY后会回送一个IGMP REPORT。

如果主机想离开一个组播组，可以有两种方式：主动离开和被动离开。主动离开就是主机发送一个IGMP LEAVE包给路由器，被动离开就是当主机收到路由器发来的IGMP QUERY后不回送IGMP REPORT。

与主机离开组播组的方式对应，在交换机上端口脱离二层组播条目的方式也有两种：超

时离开和收到IGMP LEAVE包离开。

当交换机超过一定的时间没有从一个端口收到一个组播组的IGMP REPORT包时，该端口要从对应的二层组播条目中清除，如果该二层组播条目没有了端口，则删除二层组播条目。

当交换机的fast-leave配置为ENABLE时，如果某个端口收到一个组播组的IGMP LEAVE包时，该端口从对应的二层组播条目中清除，如果该二层组播条目没有了端口，则删除此二层组播条目。

Fast-leave一般应用在一个端口下接一个主机的情况；如果一个端口下面多于一个主机，可以配置fast-leave-timeout等待时间，这样可以保证网络中组播流的连续性和可靠性。

9.2 IGMP SNOOPING 配置

9.2.1 IGMP SNOOPING 缺省配置

IGMP SNOOPING缺省是关闭的，二层硬件组播转发表处于未注册转发模式。

Fast-leave缺省是关闭的。

Fast-leave-timeout 时间为300秒。

组播组REPORT 端口的age时间缺省为300秒。

组播组QUERY端口的age时间缺省为400秒。

9.2.2 打开和关闭 IGMP SNOOPING

打开IGMP SNOOPING协议可以全局打开也可以单独打开部分VLAN；只有全局打开IGMP SNOOPING才能打开或关闭某个VLAN的IGMP SNOOPING。

打开全局IGMP SNOOPING

```
Switch#configure terminal
Switch(config)#ip igmp snooping
```

打开一个VLAN的IGMP SNOOPING

```
Switch#configure terminal
```

Switch(config)#ip igmp snooping vlan <vlan-id>

关闭全局IGMP SNOOPING

Switch#configure terminal

Switch(config)#no ip igmp snooping

关闭一个VLAN的IGMP SNOOPING

Switch#configure terminal

Switch(config)#no ip igmp snooping vlan <vlan-id>

9.2.3 配置生存时间

配置组播组的生存时间

Switch#configure terminal

Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>

Interval的单位是毫秒。

配置查询组的生存时间

Switch#configure terminal

Switch(config)#ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>

Interval的单位是毫秒。

9.2.4 配置 fast-leave

启动一个VLAN的fast-leave

Switch#configure terminal

Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

关闭fast-leave

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave vlan <vlan-id>

配置fast-leave等待时间

Switch#configure terminal

Switch(config)# ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

恢复缺省fast-leave等待时间

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave-timeout vlan <vlan-id>

9.2.5 配置 MROUTER

配置静态的查询端口

Switch#configure terminal

Switch(config)#ip igmp snooping mrouter <interface-name> vlan [vlan-id]

如果用户没有输入VLAN，那么系统会把这查询端口配置为这个端口所属的所有VLAN的MROUTER。

9.2.6 显示信息

显示IGMP SNOOPING配置信息

Switch#show ip igmp snooping

显示一个VLAN的配置信息

Switch#show ip igmp snooping vlan <vlan-id>

显示REPORT组播组的老化信息

Switch#show ip igmp snooping age-table group-membership

显示QUERY的老化信息

Switch#show ip igmp snooping age-table query-membership

显示组播组的转发信息

Switch#show ip igmp snooping forwarding-table

显示MROUTER信息

Switch#show ip igmp snooping mrouter

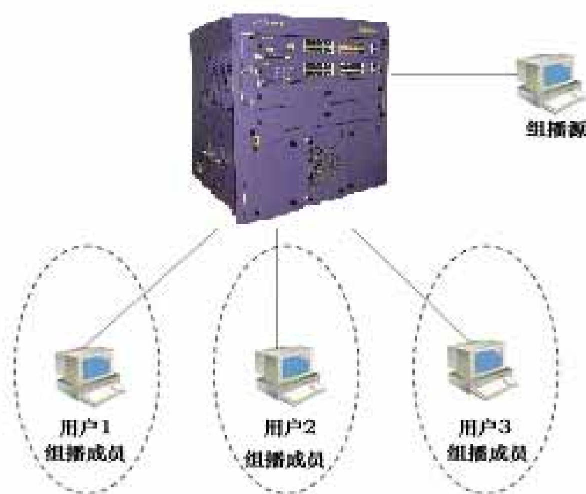
显示系统当前配置，包括IGMP SNOOPING的配置

Switch#show running-config

9.3 IGMP SNOOPING 配置示例

9.3.1 配置

在交换机上启用IGMP SNOOPING功能，用户1、用户2、用户3可加入到特定的组播组中。




```
Switch#config t
Switch(config)#ip igmp snooping
Switch(config)#vlan database
Switch(config-vlan)#vlan 200
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode access
Switch(config-ge1/1)#switchport access vlan 200
```

```
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ip igmp snooping vlan 200
Switch(config)#ip igmp snooping group-membership-timeout 60000 vlan 200
```

第10章 配置ACL

在实际的网络中，网络的访问安全是管理员非常关注的问题。iSpirit 8806交换机支持ACL过滤提供网络的访问安全。通过配置ACL规则，交换机根据这些规则对输入的数据流过滤实现网络的访问安全。

本章介绍如何配置ACL，主要包括以下内容：

- ACL资源库介绍
- ACL过滤介绍
- ACL资源库配置
- ACL过滤配置
- ACL配置示例

10.1 ACL 资源库介绍

ACL(Access list control)资源库是多组访问规则的集合，ACL资源库没有控制数据转发的功能，只是一个具有冲突排序的规则集合。ACL资源库在被应用引用后，这些应用就根据ACL资源提供的规则来控制数据的转发。ACL可以应用于端口访问过滤，服务访问过滤和QOS等等。

ACL资源库有标准IP规则组（组号1～99，1300～1999），扩展IP规则组（组号100～199，2000～2699）；，二层ACL规则组（组号700～799，1100～1199）；每一组规则内部自动进行冲突规则优先顺序排序。当用户配置一个ACL规则时，系统会根据排序规则把这条规则插入到相应的位置。

在应用时，当一个数据包通过一个端口的时候，交换机将每一条规则中的字段和数据包中相应的所有字段进行比较；当同时出现多个规则完全匹配时，最先完全匹配的一条规则生效；由这条匹配的规则来决定数据包是转发还是丢弃。所谓的完全匹配是，规则中的字段的值和数据包中相应字段的值完全相等。只有完全匹配ACL某一条规则，这规则才会作相应的deny或permit操作。

在iSpirit 8806交换机中，同一组内的规则是自动排序的。规则的自动排序相对比较复杂，在排序过程中范围大的规则排在后面，范围小的排在前面。范围的大小由规则的约束条件决定；规则的约束条件越少规则匹配的范围就越大，规则的约束条件越多规则匹配的范围就越小。规则的约束条件主要体现在地址的wildcard和一些非地址字段的个数两方面。Wildcard是bit串。IP地址是四字节，MAC地址是六字节。bits为’1’表示不需要匹配，bits为’0’表示要匹配。非地址字段是指协议类型，IP协议类型，协议端口，这些字段也隐藏了一个wildcard。他们的长度是相应字段的字节长度，因此相同的字段长度是统一的，只需计算字段的个数。Wildcard为’0’的bit越多约束条件就越多。

下面以端口访问过滤为例说明规则排序的必要性和自动排序的优点。假如用户需要拒绝源地址为192.168.0.0/16网段的地址转发，允许源地址为192.168.1.0/24网段的地址转发，可以配置以下两条规则：

access-list 1 permit 192.168.1.0 0.0.0.255－规则1

access-list 1 deny 192.168.0.0 0.0.255.255 －规则2

后面简称规则1和规则2。

这两条规则是有冲突的；因为规则2的地址包含在规则1的地址中，而且一个是deny，一个是permit；根据ACL的过滤原理，不同的顺序有不同的结果。如果要实现上述要求，上面两条规则的顺序必须是：规则1排在前面，规则2排在后面。交换机自动实现了上述的排

序功能，无论用户以怎样的先后顺序配置上述的规则，最后的顺序都是规则1排在规则2的前面。当一个源地址为192.168.1.1地址的包上来转发时，首先比较第一条规则，再往后进行比较第二条规则，两条规则都匹配，前面的生效(转发)；如果源地址为192.168.0.1时,只有第一条匹配，那么就丢弃(不转发)。如果没有进行排序，用户可能会现先配置规则2，后配置规则1；规则1排在后面，规则2排在前面。

access-list 1 deny 192.168.0.0 0.0.255.255－规则2

access-list 1 permit 192.168.1.0 0.0.0.255－规则1

因为前面的规则2包含了后面的规则1，可能会导致的情况是：完全匹配规则1的数据包也完全匹配规则2，规则2每次都会生效；而不能达到应用的需求。

在交换机中，'0.0.255.255'是Wildcard bits，bits为'1'表示不需要匹配，bits为'0'表示要匹配。由此可以看出规则2的Wildcard bits为'0.0.255.255'，需要匹配两个字节(16个bits)；规则1中，的Wildcard bits为'0 0.0.0.255'，需要匹配三个字节(24个bits)；所以规则2的规则'范围'更大，因此排在前面。在扩展IP中，排序需要考虑更多的规则字段，如IP协议类型,通信端口等等。它们的排序规则是一样的，即配置限制越多规则的'范围'就越小，反之'范围'就越大。规则的排序在后台实现，用户命令只能按用户配置的先后顺序显示。

ACL支持的过滤字段包括了源IP，目的IP，IP协议类型(如：TCP，UDP，OSPF)，源端口（如161），目的端口。对于二层ACL规则组，ACL支持的过滤字段包括了源MAC，目的MAC，VLAN，以太网类型，源IP，目的IP，IP协议类型(如：TCP，UDP，OSPF)，arp操作类型，发送者MAC，发送者IP。其中当以太网类型为IP时，过滤字段还包括IP头中的IP版本和IP头长度，且限定为0x45。当以太网类型为ARP时，过滤字段还包括ARP头中的协议、硬件地址长度及协议地址长度，且限定为0x08000604。用户可以根据不同的需要，配置不同的规则来进行访问控制。

在交换机中，一组规则可以被多个应用所应用；如：一组规则被端口访问过滤和服务访问过滤同时引用或同时被两个端口的端口访问过滤所引用。

10.2 ACL 过滤介绍

ACL过滤是在交换机的输入端口处进行的，对输入到此端口的数据流进行规则匹配实现端口的过滤。ACL过滤都是交换机的线速进行处理的，不会影响数据流的转发效率。

当交换机的某端口没有配置ACL过滤时，所有通过该端口输入的数据流不会进行规则匹配，可以通过该端口进行转发。当交换机的某端口配置了ACL过滤时，所有通过该端口的输

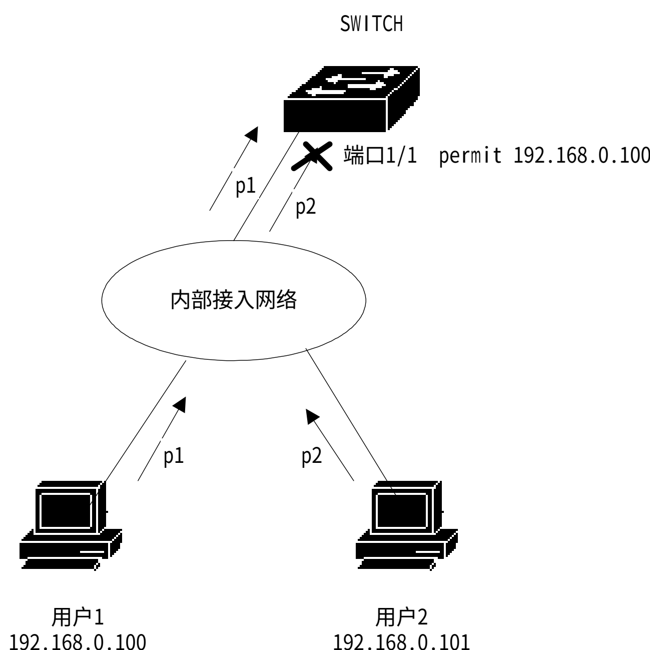
入数据流会进行规则匹配，匹配的规则的动作如果是permit，该数据流允许转发，如果是deny，该数据流不允许转发，丢弃。

在配置端口的ACL过滤时，一个端口可以选择多个ACL规则组，选择后该组规则导入到端口的FFP中，如果该组规则中没有拒绝或允许所有IP协议包的规则，则写入FFP时会加一条拒绝所有IP协议的规则。如果该组规则中有二层过滤的ARP协议包的规则，但没有拒绝或允许所有二层过滤的ARP协议包的规则，则写入FFP时会加一条拒绝所有二层过滤的ARP协议包的规则。注意，这里提到的二层过滤的ARP协议包，要求它的ARP头中的协议、硬件地址长度及协议地址长度一定为0x08000604。FFP处理IP协议包的规则与处理二层过滤的ARP协议包的规则互不冲突。当ACL资源库的规则变化后，写入FFP中的规则也会自动的变化。

例如一组规则中只有一条规则：access-list 1 permit 192.168.1.0 0.0.0.255，缺省会隐藏一条拒绝所有IP协议包的规则，实际上会有两条规则导入到端口的FFP。在数据流过滤时，只有源地址从192.168.1.0到192.168.1.255的数据流可以通过该端口进行转发，所有其它的数据流被过滤掉。对于二层过滤的ARP协议包的规则，例如一组规则中只有一条规则：access-list 1100 permit host 0011.5B31.F2C4 host 0011.5B3A.D043 1 arp any any any，缺省会隐藏一条拒绝所有二层过滤的ARP协议包的规则，实际上会有两条规则导入到端口的FFP。在数据流过滤时，只有MAC地址从0011.5B31.F2C4到0011.5B3A.D043且属于VLAN 1的数据流可以通过该端口进行转发，所有其它的二层过滤的ARP协议的数据流被过滤掉。

例如一组规则中有两条规则：access-list 1 deny 192.168.1.0 0.0.0.255和access-list 1 permit any。此时有一条允许所有IP协议包的规则，这时不存在隐藏的规则，实际上会有两条规则导入到端口的FFP。在数据流过滤时，只有源地址从192.168.1.0到192.168.1.255的数据流被过滤掉，所有其它的数据流被可以进行转发。

如下图是一个ACL过滤的例子。交换机的端口1/1选择一个ACL规则组1，该组规则中只有一条规则access-list 1 permit 192.168.0.100。在交换机的端口1/1下，有两个用户想从该端口接入网络，用户1的IP地址是192.168.0.100，用户2的IP地址是192.168.0.101。只有用户1可以通过交换机的端口1/1接入网络，用户2不能通过交换机的端口1/1接入网络。用户1发出来的数据流p1可以通过交换机的端口1/1转发，而用户2发出来的数据流p2则在交换机的端口1/1处丢弃。



多个端口做ACL过滤时可以选用同一个ACL规则组，使用相同的过滤规则。

不管是一组规则还是多组规则被一个端口引用，它们都会自动的进行排序，即使是两组规则之间的排序有交叉的情况。

当用户引用了一组规则后，如果这组规则发生变化，那么引用了这组规则的端口会自动响应用户的配置；不需要重新来配置这个端口的引用。

10.3 ACL 资源库配置

交换机缺省没有任何规则。

在交换机中的资源库支持四类ACL规则：标准IP规则，扩展IP规则， MAC IP协议规则，MAC ARP协议规则。下面分四类规则来介绍ACL的配置。

在交换机中的资源库支持三类ACL规则：标准IP规则，扩展IP规则，扩展MAC规则。下面分三类规则来介绍ACL的配置。

标准IP规则：标准IP规则是通过源IP地址来控制数据包的转发。

命令形式：access-list <groupId> {deny | permit} <source>

参数说明：

groupId：访问控制列表组号，标准IP ACL 支持从1到199组或1300到1999。

deny/permit：如果完全匹配，则拒绝或允许该数据包转发。

source：源IP有三种输入方式：

A.B.C.D wildcard 可以控制来自一个网段的IP地址；

any 相当于A.B.C.D 255.255.255.255

host A.B.C.D相当于A.B.C.D 0.0.0.0

wildcard：决定哪些bits需要匹配，’0’表示需要匹配，’1’表示不需要匹配。

扩展IP规则：扩展IP规则是标准IP规则的扩展，可以通过源IP，目的IP，IP协议类型和服务端口来控制数据包的转发。

命令形式：access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort]

参数说明：

groupId：访问控制列表组号，扩展IP ACL 支持从100到199组或2000到2699。

deny/permit：如果完全匹配，则拒绝或允许该数据包转发。

protocol：在IP层之上的协议类型，如：icmp，tcp，udp等，也可以输入相应的数字6(tcp)。如果不需要对这些协议进行控制，可以输入ip或0。

source：源IP有三种输入方式：

1)A.B.C.D wildcard 可以控制来自一个网段的IP地址；

2)any 相当于A.B.C.D 255.255.255.255

3)host A.B.C.D相当于A.B.C.D 0.0.0.0

srcPort：是对于protocol为tcp或udp的情况，可以控制数据包的源端口，输入方式可以是一些熟悉的端口服务名称，如：www也可以是数字，如80。

destination：目的IP有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的IP地址；

2) any 相当于A.B.C.D 255.255.255.255

3) host A.B.C.D相当于A.B.C.D 0.0.0.0

destPort：是对于protocol为tcp或udp的情况，可以控制数据包的目的端口，输入方式和srcPort相同。

MAC IP协议规则：MAC IP协议规则是通过源MAC，目的MAC，VLAN，以太网类型（IP），源IP，目的IP，IP协议类型来控制数据包的转发。

命令形式：access-list <groupId> {deny | permit} <source mac> <destination mac> <vid> ip <protocol> <source> <destination>

参数说明：

groupId：访问控制列表组号，MAC IP协议规则 ACL 支持从700到799组。

deny/permit：如果完全匹配，则拒绝或允许该数据包转发。

source mac：源MAC有三种输入方式：

1)HHHH.HHHH.HHHH wildcard 可以控制某些字段相同的一组MAC地址；

2)any 相当于HHHH.HHHH.HHHH FFFF.FFFF.FFFF；

3)host HHHH.HHHH.HHHH相当于HHHH.HHHH.HHHH 0000.0000.0000。

destination mac：目的MAC有三种输入方式：

1)HHHH.HHHH.HHHH wildcard 可以控制某些字段相同的一组MAC地址；

2)any 相当于HHHH.HHHH.HHHH FFFF.FFFF.FFFF；

3)host HHHH.HHHH.HHHH相当于HHHH.HHHH.HHHH 0000.0000.0000。

vid：VLAN ID。

protocol：在IP层之上的协议类型，如：icmp，tcp，udp等，也可以输入相应的数字6(tcp)。如果不需要对这些协议进行控制，可以输入ip或0。

source：源IP有三种输入方式：

1)A.B.C.D wildcard 可以控制来自一个网段的IP地址；

2)any 相当于A.B.C.D 255.255.255.255

3)host A.B.C.D相当于A.B.C.D 0.0.0.0

destination：目的IP有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的IP地址；

2) any 相当于A.B.C.D 255.255.255.255

3) host A.B.C.D相当于A.B.C.D 0.0.0.0

MAC ARP协议规则：MAC ARP协议规则是通过源MAC，目的MAC，VLAN，以太网类型（ARP），ARP操作类型，发送者MAC，发送者IP来控制数据包的转发。

命令形式：access-list <groupId> {deny | permit} <source mac> <destination mac> <vid> arp <ar_op> <sender mac> <sender ip>

参数说明：

groupId：访问控制列表组号，MAC ARP协议规则 ACL 支持从1100到1199组。

deny/permit：如果完全匹配，则拒绝或允许该数据包转发。

source mac：源MAC有三种输入方式：

1)HHHH.HHHH.HHHH wildcard 可以控制某些字段相同的一组MAC地址；

2)any 相当于HHHH.HHHH.HHHH FFFF.FFFF.FFFF；

3)host HHHH.HHHH.HHHH相当于HHHH.HHHH.HHHH 0000.0000.0000。

destination mac：目的MAC有三种输入方式：

1)HHHH.HHHH.HHHH wildcard 可以控制某些字段相同的一组MAC地址；

2)any 相当于HHHH.HHHH.HHHH FFFF.FFFF.FFFF；

3)host HHHH.HHHH.HHHH相当于HHHH.HHHH.HHHH 0000.0000.0000。

vid：VLAN ID。

ar_op：arp操作类型：request表示请求类型，reply表示应答类型，any表示任何类型。

sender mac：发送者MAC有三种输入方式：

1)HHHH.HHHH.HHHH wildcard 可以控制某些字段相同的一组MAC地址；

2)any 相当于HHHH.HHHH.HHHH FFFF.FFFF.FFFF；

3)host HHHH.HHHH.HHHH相当于HHHH.HHHH.HHHH 0000.0000.0000。

sender ip：发送者IP有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的IP地址；

2) any 相当于A.B.C.D 255.255.255.255

3) host A.B.C.D相当于A.B.C.D 0.0.0.0

其他命令列表：

show access-list [groupId]

显示当前ACL中配置的规则列表。如果输入了groupId则当前组的规则列表；否则显示所有的规则列表。

no access-list <groupId>

删除指定的规则列表。groupId组的所有规则。

10.4 ACL 过滤配置

交换机缺省所有的端口都没有做ACL过滤。

命令列表：

access-group <groupId>

模式：二层接口配置模式

参数：

groupId：和端口绑定的ACL组号

功能：配置ACL端口过滤。

注意：如果上面的命令配置失败或无效，可能有下面的原因：

ACL组中的规则太多或FFP被QoS等其它应用占用。

显示ACL端口过滤配置

show acccess-group

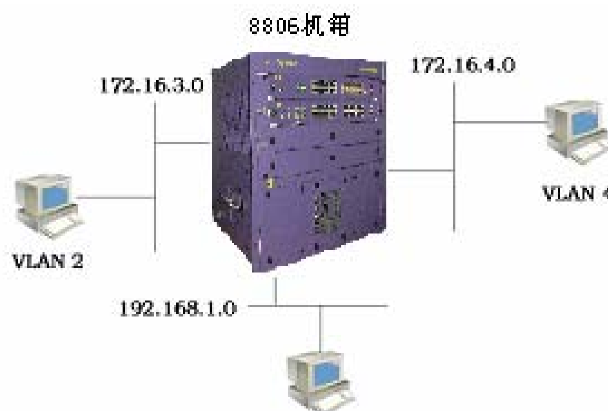
删除当前端口和ACL端口过滤相关的配置

no acl-filter <groupId>

10.5 ACL 配置示例

1、配置

一个交换机连接三个子网，设计ACL， 阻塞源地址为192.168.1.0 网络地址。而允许其他网络地址的通信流量通过。192.168.1.0 网段连接到8806 的1/1 端口。



在交换机上配置如下：

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config)#interface ge1/1
Switch(config-ge1/1)#swithport mode access
```

```
Switch(config-ge1/1)#switchport access vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
Switch(config)#interface ge1/2
Switch(config-ge1/2)#swithport mode access
Switch(config-ge1/2)#switchport access vlan 3
Switch(config)#interface vlan3
Switch(config-vlan2)#ip add 172.16.3.1/24
Switch(config)#access-list 10deny 192.168.1.0 0.0.0.255
Switch(config)#access-list 10 permit any
Switch(config)#interface ge1/2
Switch(config-ge1/1)#access-group 10
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#access-group 10
```

2、排错

在配置访问控制列表之前确定所有ip 之间都是通的，然后再添加访问控制列表。这条访问控制列表阻塞的是源地址为192.168.1.0 网段的IP 数据流通过交换机。注意子网反码的写法。用show access-list 命令列出访问控制列表进行查看，一定要注意源地址和目的地址不要写反。然后进行访问控制列表的查看。而且默认访问控制列表最后都有一条隐含的deny any 的语句，如果想让其他都通过的话，需要添加一条permit any 的语句，否则都不能够通过。

第11章 配置QOS

本章主要包括以下内容：

- QOS 介绍
- QOS 配置
- QOS 配置示例

11.1 QOS 介绍

11.1.1 QOS 概述

使用iSpirit 8806交换机的QoS功能，您能够让通过交换机转发的重要的数据流得到优先的处理，并对一些数据流进行带宽限制，使您的网络的带宽利用更加合理，网络性能变得可预测。

iSpirit 8806交换机实现了基于IETF标准的DiffServ体系结构的QoS功能，在QoS域的边界对数据流进行分类，给每个数据流打上一个DSCP值，在QoS域内根据数据流的DSCP值进行优先级处理。iSpirit 8806交换机不仅实现了DiffServ的QoS，还实现了802.1p的QoS以及早期应用的比较多的IP Precedence的QoS。

在QoS域的边界，根据交换机的QoS配置策略把不同的数据流打上不同的优先级标记，也就是业务类标记，在QoS域内所有的设备根据业务类标记对数据流进行转发。这样，QoS域内的设备不需要执行复杂的流分类和复杂的QoS策略，只需要使用业务类标记进行优先级处理。

当数据流进入QoS域的边界，QoS域边界的交换机不仅会把数据流归并到业务类中，还可以对业务类进行带宽处理，比如进行带宽资源的预留或做带宽的限制，这样可以保证QoS域中的带宽资源得到合理的利用。

为了保证网络中端到端的服务质量保证，在QoS域中的所有设备都需要具有相应的QoS功能。QoS域边界的交换机需要具有强大的QoS功能，能够根据IP数据包的多个字段对数据流进行分类，能够根据业务类进行带宽分配，能够支持多种调度策略。QoS域内的交换机只需要根据业务类标记进行优先级处理就行了。iSpirit 8806交换机能够作为域边界交换机，也能够作为域内交换机。

11.1.2 QOS 模型

如图显示了QoS模型。在输入端口实现了classification，policing，mark，介绍如下：

业务分类（classification）：对接收到IP数据包进行业务分类，生成一个内部DSCP值，为做QoS策略做准备。

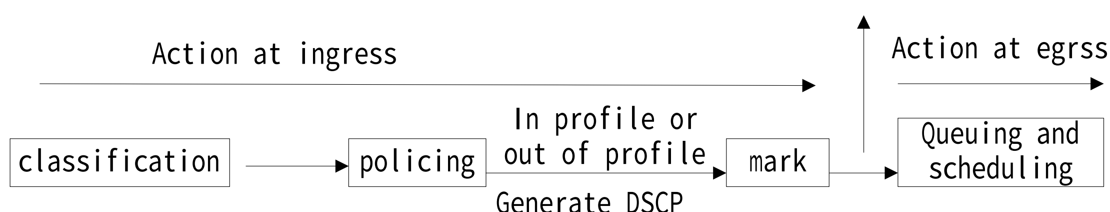
QoS策略（policing）：根据业务分类得到的内部DSCP值进行QoS处理，包括带宽限制，映射到一个优先级队列，产生业务类标记值。

Mark：对Out of Profile的数据流进行丢弃处理，对In Profile的数据流看是否需要修改数据流的业务类标记。

在输出端口实现了Queuing和Scheduling，介绍如下：

存入队列（Queuing）：根据QoS策略得到的结果把IP数据包放入对应的输出优先级队列中进行缓存。

调度（Scheduling）：根据调度策略对存入队列中的IP数据包进行优先级处理并发送出去。



11.1.3 QOS 业务分类

业务分类用于区分不同的数据流，根据数据流的一个或多个字段匹配进行分类，映射成一个内部DSCP值。只有启用QoS的交换机端口收到数据包才会进行业务分类，如果一个端口没有启用QoS，则不进行业务分类，采用best-effort的方法进行转发。

对于QoS信任端口，业务分类比较简单，直接根据业务类标记进行分类，映射成内部DSCP值。

对于Trust COS端口，直接根据数据帧的TAG标记中的三位优先级进行分类，根据COS-DSCP映射表生成内部DSCP值，所有的数据流根据三位优先级最多可分成8类。注意：如果数据帧没有TAG标记，则认为其COS优先级值为0，而不是端口缺省优先级（PPD-COS），数据帧如果从输出端口带标记发送出去，则其标记的COS优先级为输入端口的缺省优先级。

对于Trust Ip-precedence端口，直接根据IP数据包的TOS字段的最高三位进行分类，根据PREC-DSCP映射表生成内部DSCP值，所有的数据流根据三位Ip-precedence值最多可分成8类。

对于Trust DSCP端口，直接根据IP数据包的TOS字段的最高六位进行分类，根据DSCP-DSCP映射表生成内部DSCP值，所有的数据流根据六位DSCP值最多可分成64类。

对于QoS非信任端口，业务分类比较复杂，需要根据数据流的一个或多个字段进行分类，多个不同的数据流可以映射为一个业务类。iSpirit 8806交换机提供了CLASS和POLICY配置模式对数据流进行分类，在CLASS模式中，选择哪些数据流组成一个业务类，在POLICY

模式中，把每个业务类映射为一个内部DSCP值，一个POLICY可以包括一个或多个CLASS。

在CLASS模式中，可以有以下几种选择组成一个业务类：

选择一个或多个COS（最多8个）组成一个业务类，称为COS业务类。

选择一个或多个IP Precedence（最多8个）组成一个业务类，称为PREC业务类。

选择一个或多个DSCP（最多8个）组成一个业务类，称为DSCP业务类。

选择一个（只能有一个）ACL组组成一个业务类，称为ACL业务类。

对于基于ACL的业务分类，每个ACL组组成一个业务类，一个ACL组中有1条到128条规则，只有动作为permit的规则在QoS中才会生效，而动作为deny的规则在QoS中是无效的。ACL组可以是标准IP组，扩展IP组，扩展MAC组。

在POLICY模式中，每个业务类可以映射成一个业务类标记值，业务类标记值再根据映射表生成一个内部DSCP值。如下：

业务类映射成COS业务类标记值，根据COS-DSCP映射表生成内部DSCP值。

业务类映射成IP Precedence业务类标记值，根据PREC-DSCP映射表生成内部DSCP值。

业务类映射成DSCP业务类标记值，根据DSCP-DSCP映射表生成内部DSCP值。

11.1.4 QOS 策略

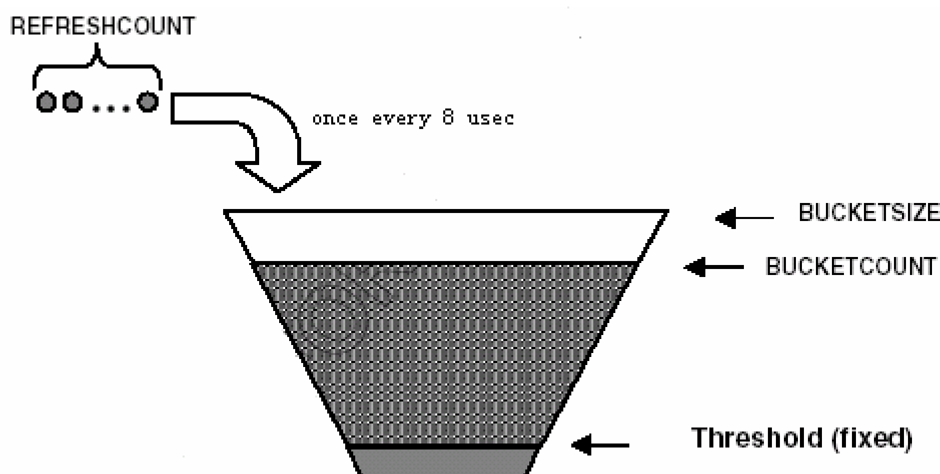
QoS策略包括policing和mark两个部分。当数据流分类后，需要采用一定的QoS策略对业务类进行QoS处理。QoS策略主要包括以下内容：

决定业务类的带宽限制，是否在带宽限制内还是超过带宽限制。

决定业务类的优先级队列。

决定业务类标记，是否需要修改数据包，如何修改。

iSpirit 8806交换机的每个输入端口都支持对每个数据流进行带宽限制，可以实现业务类的带宽限制处理，采用漏斗算法进行带宽限制处理，如图所示。漏斗的深度bucketsize指的是能支持的最大突发数据流的大小，即burstsize。当有匹配的数据流从输出端口流出时，相当与从漏斗流出，bucketcount往下移动，当bucketcount处于threshold的下方时，此时从输入端口流入的匹配数据流被限制住，处于Out of Profile状态。每隔8us系统根据设定的带宽限制值定时往漏斗中加refreshcount的流量，bucketcount往上升，当处于threshold的上方时，数据流又允许流出，此时处于In Profile状态。当某个业务类处于Out of Profile状态时，丢弃后续输入的数据流，如果处于In Profile状态时，做进一步的处理。



当数据流处于In Profile状态时，可以做进一步处理，下一步要决定业务类送入输出端口的优先级队列。每一个业务类通过业务分类的步骤都得到一个内部DSCP值，通过DSCP-QUEUE映射表可以得到输出端口的优先级队列。iSpirit 8806交换机的每个输出端口支持8个优先级队列。

业务类的业务类标记值在业务分类阶段已经得到，有三种业务类标记类型：COS业务类标记，IP Precedence业务类标记和DSCP业务类标记，在输出端口需要修改数据包对应字段，把业务类标记加在数据包中。

QoS信任端口和非信任端口在QoS策略的处理上有很大的不同，QoS信任端口只需要决定数据流的优先级队列，不需要做带宽限制和生成业务类标记值，也不修改IP数据包头。而QoS非信任端口则根据系统端口的配置情况进行QoS策略处理，确定业务类标记值，决定优先级队列是必须要做的，可以配置不做带宽限制处理。

11.1.5 QOS 调度

iSpirit 8806交换机的输出端口支持8个优先级队列，队列1优先级最低，队列8优先级最高。当数据流缓存在输出队列中后，输出端口需要根据配置的QoS调度方法对数据流做优先级处理，决定数据流的发送次序。iSpirit 8806交换机的输出端口支持3种QoS调度方法，如下：

严格优先级调度（SPQ）：严格按照优先级对数据流进行调度，只有高优先级队列中的所有数据流发送出去后，才发送低优先级队列中的数据流。这种方法的缺点是低优先级队列中的数据流可能等待很长时间才得到处理。

循环调度（RR）：队列1到队列8的数据流按照相同的权重进行调度，实际上队列1到队列8的优先级是一样的。这种方法的缺点是不能保证重要数据的服务质量，实际上就跟没做QoS是一样的。

加权循环调度（WRR）：可以根据实际应用需要配置队列的权重，输出端口按照配置的队列权重对数据流进行调度。这种方法可以解决SPQ和RR调度方法的不足，可以保证重要数据的服务质量。

11.2 QOS 配置

在做QoS配置之前，需要注意以下两点：

管理员先要了解网络中的实际应用以及交换机在QoS域中的位置,根据实际网络的需求做QoS配置。

iSpirit 8806交换机根据每个端口启用QoS，在启用QoS之前，要了解本端口的FFP的使用情况，本端口是否设置了802.1x和ACL过滤，本系统是否启用了IGMP SNOOPING协议等。

11.2.1 QOS 缺省配置

iSpirit 8806交换机缺省情况下所有的端口都没有启用QoS，所有的数据流以best-effort的方法转发。

端口的缺省COS优先级为0。

COS-DSCP映射表缺省如下图。

COS值	0	1	2	3	4	5	6	7
内部DSCP值	0	8	16	24	32	40	48	56

PREC-DSCP映射表缺省如下图。

IP Precedence值	0	1	2	3	4	5	6	7
内部DSCP值	0	8	16	24	32	40	48	56

DSCP-DSCP映射表缺省如下图。

DSCP值	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
内部DSCP值	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

DSCP值	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
内部DSCP值	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

DSCP值	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
内部DSCP值	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47

DSCP值	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
内部DSCP值	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63

DSCP-QUEUE映射表缺省如下图。

内部DSCP值	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
队列QUEUEP值	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2

内部DSCP值	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
队列QUEUE值	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4

内部DSCP值	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
队列QUEUE值	5	5	5	5	5	5	5	5	6	6	6	6	6	6	6	6

内部DSCP值	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
队列QUEUE值	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8

输出端口的QoS调度方法缺省为严格优先级调度（SPQ）。

11.2.2 配置 QOS 映射表

所有的QoS映射表的配置命令都在CLI　CONFIG模式下输入，显示命令都在CLI全局模式下输入

下面的两条命令用于配置和显示COS-DSCP映射表：

qos cos-dscp <cos-value> <internal-dscp-value>

show qos cos-dscp

例如把COS值0映射成内部DSCP值40：

Switch(config)qos cos-dscp 0 40

Switch# show qos cos-dscp

下面的两条命令用于配置和显示PREC-DSCP映射表：

qos prec-dscp <ip-precendence-value> <internal-dscp-value>

show qos prec-dscp

例如把IP Precedence值0映射成内部DSCP值40：

Switch(config)qos prec-dscp 0 40

Switch# show qos prec-dscp

下面的两条命令用于配置和显示DSCP-DSCP映射表：

qos dscp-dscp <dscp-value> <internal-dscp-value>

show qos dscp-dscp

例如把DSCP值0映射成内部DSCP值40：

Switch(config)qos dscp-dscp 0 40

Switch# show qos dscp-dscp

下面的两条命令用于配置和显示DSCP-QUEUE映射表：

qos interdscp-queue <internal-dscp-value> <queue-id>

show qos interdscp-queue

例如把内部DSCP值40映射成队列2：

Switch(config)qos interdscp-queue 40 2

Switch# show qos interdscp-queue

注意：对映射表的配置只对后续端口启动的QoS有效，对于已经启动了QoS的端口，使用的是修改前的映射表。

11.2.3 配置 QOS 信任端口

QoS信任端口包括Trust COS端口，Trust Ip-precedence端口和Trust DSCP端口。QoS信任端口的配置在Interface配置模式下输入，显示命令在CLI全局模式下输入。

下面的命令用于配置Trust COS端口：

qos trust cos

例如端口1/2配置成Trust COS端口：

Switch(config-ge1/2)# qos trust cos

Switch# show qos

下面的命令用于配置Trust Ip-precedence端口：

qos trust ip-precedence

例如端口1/2配置成Trust Ip-precedence端口：

Switch(config-ge1/2)# qos trust ip-precedence

Switch# show qos

下面的命令用于配置Trust DSCP端口：

qos trust dscp

例如端口1/2配置成Trust DSCP端口：

Switch(config-ge1/2)# qos trust dscp

Switch# show qos

下面的命令用于清除端口的QoS配置：

no qos

例如端口1/2，清除端口的QoS配置：

Switch(config-ge1/2)# no qos

Switch# show qos

注意：

如果配置QoS信任端口不成功，有三种可能性：该端口已经配置了QoS（需要先清除端口的QoS配置，再对端口做QoS配置）、该端口的FFP被ACL过滤或其它功能占用过多。Trust COS需要占用FFP的RULE表中的8个条目，Trust Ip-precedence需要占用FFP的RULE表中的8个条目，Trust DSCP需要占用FFP的RULE表中的64个条目。

一个端口可以在配置为QoS信任端口的同时又做ACL过滤，可以先配置ACL过滤，再配置QoS信任端口，也可以先配置QoS信任端口，再配置ACL过滤。

11.2.4 配置 QOS 业务类

QoS业务类包括四种：COS业务类、PREC业务类、DSCP业务类和ACL业务类。

在选择一个业务之前需要创建一个QoS类，在CONFIG模式下输入下面的命令创建一个QoS类，class-id的范围从1到1000。可以给QoS类取一个名字用于标识该类：

qos class <class-id> name <class-name>

例如创建一个QoS类，class-id为3，名字为abc：

Switch(config)# qos class 3 name abc

Switch# show qos class 3

在某个CLASS下，给QoS类选择一种业务流。

下面的命令给QoS类选择COS业务流，形成COS业务类，最多可以输入8个COS值，如果输入的值相同，相同的值认为是一个：

qos class <class-id> match cos <cos-value> [cos-value] …

下面的命令给QoS类选择IP Precedence业务流，形成PREC业务类，最多可以输入8个IP Precednece值，如果输入的值相同，相同的值认为是一个：

qos class <class-id> match ip-precedence <ip-precedence-value> [ip-precedence-value] …

下面的命令给QoS类选择DSCP业务流，形成DSCP业务类，最多可以输入8个DSCP值，如果输入的值相同，相同的值认为是一个：

qos class <class-id> match dscp <dscp-value> [dscp-value] …

下面的命令给QoS类选择ACL业务流，形成ACL业务类，一个QoS类只能选择一个ACL组，选择的ACL组必须存在：

qos class <class-id> match acl <acl-id>

例如一个QoS类3选择DSCP值20、40，45、60作为一个DSCP业务类：

Switch(config)# qos class 3 match dscp 20 40 45 60

Switch# show qos class 3

在CONFIG模式下输入下面的命令删除一个QoS业务类：

no qos class <class-id>

例如删除业务类3：

Switch(config)# no qos class 3

Switch# show qos class 3

注意：

一个QoS类只能是COS业务类、PREC业务类、DSCP业务类和ACL业务类中的一种。

一个QoS业务类可以被多个Policy引用。当一个QoS业务类被一个或多个Policy引用时，这个QoS业务类不能被删除和修改。

11.2.5 配置 QOS 策略

iSpirit 8806交换机总共支持256个QoS策略，每一个QoS策略可以选择一个或多个QoS业务类，对每一个QoS业务类配置对应的策略。

在CONFIG模式下输入下面的命令选择一个QoS策略，在选择的策略下再选择一个业务类，对选择的业务类配置策略，包括配置业务类标记和配置带宽限制。

业务类标记包括三种：COS业务类标记、IP Precedence业务类标记和DSCP业务类标记。

下面的命令对业务类配置COS业务类标记：

qos policy <policy-id> class <class-id> set cos <cos-value>

下面的命令对业务类配置IP Precedence业务类标记：

qos policy <policy-id> class <class-id> set ip-precedence <ip-precedence-value>

下面的命令对业务类配置DSCP业务类标记：

qos policy <policy-id> class <class-id> set dscp <dscp-value>

一个业务类在做QoS策略配置时，可以配置带宽限制策略，也可以不配置。如果配置带宽限制时，最小带宽限制值为4 kbytes/s，粒度为64kbps。下面的命令在POLICY CLASS下配置业务类的带宽限制：

qos policy <policy-id> class <class-id> meter <bandwidth-value> <burst-size>

下面的命令用于取消业务类的带宽限制，即业务类不做带宽限制策略：

no qos policy <policy-id> class <class-id> meter

在CONFIG模式下输入下面的命令清除QoS策略中的一个或所有的业务类，如果不输入class-id，则清除QoS策略中的所有的业务类，如果输入class-id，则清除指定的业务类：

no qos policy <policy-id> [class-id]

下面举一个QoS策略配置的示例：

Policy 2中包括两个业务类：Class 3和Class 4。Class 3和Class 4都是ACL业务类，分别匹配IP标准ACL组3和IP扩展ACL组103。Class 3配置DSCP业务类标记，值为40，限制refreshcount到2048kbps，限制burstsize到512kbytes/s，Class 4配置IP Precedence业务类标记，值为6，不限制带宽。配置如下：

Switch(config)#qos class 3 match acl 3

（业务类3为ACL业务类，选择ACL组3，假设ACL组3已经存在）

Switch(config)#qos class 4 match acl 103

（业务类4为ACL业务类，选择ACL组103，假设ACL组103已经存在）

Switch# show qos class

（显示业务类配置情况）

Switch(config)#qos policy 2 class 3 set dscp 40

Switch(config)#qos policy 2 class 3 meter 2048 512 （策略2选择业务类3，对业务类3进行QoS策略配置，设置DSCP业务类标记值，设置业务类3的带宽限制）

Switch(config)#qos policy 2 class 4 set ip-precedence 6（策略2选择业务类4，对业务类4进行QoS策略配置，设置IP Precedence业务类标记值）

Switch# show qos policy 2（显示Policy 2的配置）

注意：

一个QoS策略可以选择一个或多个QoS业务类，最多可以选择128个业务类。

一个QoS策略中的一个业务类只能配置COS业务类标记值、IP Precedence业务类标记值和DSCP业务类标记值中的一种。

一个QoS策略可以被一个或多个非信任端口引用。

当一个QoS策略被一个或多个非信任端口引用时，该QoS策略不能被删除和修改。

11.2.6 配置 QOS 非信任端口

配置QoS非信任端口实际上就是端口选择一个QoS策略。下面的命令用于在Interface模式下配置非信任端口，选择的policy-id必须存在。

qos service-policy <policy-id>

例如端口1/2选择Policy 2配置非信任端口：

Switch(config-ge1/2)# qos service-policy 2

Switch# show qos

如果非信任端口配置不成功，可能有以下几种情况：

该端口已经配置成QoS信任端口或QoS非信任端口。

选择的QoS策略不存在。

该端口已经绑定了一个或多个IP地址。

该端口的FFP的RULE表空间不足，可能是：该端口已经做了ACL过滤或QoS分类的数据流过多。每个端口的FFP的RULE表的空间有128个条目。

该端口的FFP的METER表空间不足，可能是QoS策略中做带宽限制的业务类太多，超过了128个，这种情况比较少出现。FFP的METER表的空间有128个条目。

注意：

QoS策略中的两个或多个ACL业务类，每个ACL业务类匹配一个ACL组，这些组中有相同的两条过滤规则。则先配置的业务类生效。

举例如下：

ACL组2配置2条规则：

Switch(config)# access-list 2 permit 192.168.0.0 0.0.0.255

Swtich(config)# access-list 2 permit 192.168.1.0 0.0.0.255

ACL组3配置1条规则，该条规则与ACL组2中的1条规则相同

Switch# access-list 3 permit 192.168.0.0 0.0.0.255

QoS类2配置为ACL业务类，ACL组为2：

Switch(config)# qos class 2 match acl 2

QoS类3配置为ACL业务类，ACL组为3：

Switch(config)# qos class 3 match acl 3

配置QoS策略2，选择业务类2和业务类3：

Switch(config)# qos policy 2 class 2 set dscp 30

Switch(config)# qos policy 2 class 3 set dscp 40

设置端口1/2为非信任端口，选择Policy 2：

Switch(config-ge1/2)# qos service-policy 2

此时QoS非信任端口qos policy 2 class 2 set dscp 30配置成功，业务类3配置不生效。用户在配置时不同的业务类匹配的ACL组最好不要有相同的规则。

下面的命令在Interface模式下清除端口的QoS配置：

no qos

例如端口1/2原来配置为非信任端口，选择了Policy 2作为其策略，现在清除端口的QoS配置：

Switch(config-ge1/2)# no qos

Switch# show qos

注意：

每个端口只能配置为Trust COS, Trust IP_Precedence、Trust DSCP和非信任端口中的一种，如果配置为非信任端口，只能选择一个QoS策略。

一个端口可以配置QoS非信任端口的同时做ACL过滤，也可以做ACL过滤的同时配置QoS非信任端口。如果对一条规则既做了QOS配置，又做了ACL配置，配置的结果可以看成两种配置的叠加。

一个端口配置为QoS非信任端口时，QoS策略中的ACL业务类的 “ permit ” 动作的ACL

规则会写入FFP，“ deny ”动作的ACL规则不会写入FFP，也就是说“ deny ”动作的ACL规则不会对数据流做QoS。

如果一个QoS策略中的两个或多个的业务类有相同的匹配值，则第一个配置的业务类中的匹配值做QoS，后面配置的相同的匹配值不会做QoS。如一个COS业务类有一个匹配的COS值5，另一个COS业务类也有一个匹配的COS值5，则第一个配置的COS值为5的做QoS。建议用户在配置时不要配置重复的匹配值。

11.2.7 配置 QOS 调度方法

一个端口的输出端做QoS调度，iSpirit 8806交换机支持3种调度方法：严格优先级调度（SPQ），循环调度（RR），加权循环调度（WRR）。对于WRR，每个优先级队列必须有一个权重，队列1到8的缺省权重分别为1、2、3、4、5、6、7、8，可以对优先级队列的权重进行配置，权重的范围是1到15。

在PORT RANGE模式下配置端口的QoS调度方法。

下面的命令配置端口的QoS的调度方法为SPQ：

qos schedule spq

下面的命令配置端口的QoS的调度方法为RR：

qos schedule rr

下面的命令配置端口的QoS的调度方法为WRR，可以不输入权重，如果输入权重，必须输入队列1到8的权重：

qos schedule wrr [<queue1-weight> <queue2-weight>…<queue8-weight>]

例如端口1/2配置为WRR调度方法，队列1到8的权重分别为1、3、5、9、11、13、14、15：

Switch(config-ge1/2)# qos schedule wrr 1 3 5 9 11 13 14 15

Switch# show qos schedule

11.3 QOS 配置示例

11.3.1 配置

在交换机上作如下配置：

设置端口1/2为Trust COS端口。配置Policy 2，策略内容为对网段192.168.0.1/24和网段192.168.1.1/24的包设置TOS优先级为6，对包中DSCP值为20、40、45、60的包，设置它的DSCP值为40，并且设置带宽为2048kbps，burstsize为512kbytes。。设置端口1/3为非信任端口，选择Policy 2。设置端口1/4为WRR调度方法，队列1到8的权重分别为1、3、5、7、9、11、13、15。

```
Switch# configure terminal
Switch(config)# interface ge1/2
Switch(config-ge1/2)# qos trust cos
Switch(config-ge1/2)# exit
Switch(config)# access-list 2 permit 192.168.0.0 0.0.0.255
Swtich(config)# access-list 2 permit 192.168.1.0 0.0.0.255
Switch(config)# qos class 2 match acl 2
Switch(config)# qos class 3 match dscp 20 40 45 60
Switch(config)# qos policy 2 class 2 set ip-precedence 6
Switch(config)# qos policy 2 class 3 set dscp 40
Switch(config)# qos policy 2 class 3 meter 2048 512
Switch(config)# interface ge1/3
Switch(config-ge1/3)# qos service-policy 2
Switch(config-ge1/3)# interface ge1/4
Switch(config-ge1/4)# qos schedule wrr 1 3 5 7 9 11 13 15
```

第12章 配置IP路由

路由是三层交换机的重要功能之一，能够实现在不同的IP网段间的数据转发。路由的概念很宽泛，以三层接口和ARP协议为基础，包括静态路由和动态路由。静态路由是用户手工配置的路由，而动态路由是通过动态路由协议自动学习到的路由。动态路由协议在后面的章节中介绍。

本章主要包括以下内容：

- 配置VLAN接口
- 配置ARP
- 配置静态路由
- 路由冗余备份
- 配置策略路由
- IP路由配置示例

12.1 配置 VLAN 接口

在交换机中，每个三层接口都是依附在某个VLAN之上的，所以三层接口又称为VLAN接口。VLAN接口的创建和删除是用户在创建和删除VLAN时自动完成的，当用户创建一个VLAN时，系统自动创建与该VLAN对应的VLAN接口，当用户删除一个VLAN时，系统自动删除与该VLAN对应的VLAN接口。交换机支持512个VLAN接口，对于4K个VLAN，只能在512个VLAN上创建VLAN接口。

每个VLAN接口都有一个名称，VLAN接口的名称是字符串“vlan”后接VLAN ID号，如VLAN 1的三层接口的名称为“vlan1”，VLAN 4094的三层接口的名称为“vlan4094”。

与端口一样，VLAN接口也有管理状态和链路状态。目前交换机不提供VLAN接口的管理状态的配置，只要VLAN接口创建好了，VLAN接口的管理状态总是UP。VLAN接口的链路状态是与该接口对应的VLAN所包含的端口相关的，只要VLAN内的一个端口的链路状态是RUNNING，则该VLAN接口的链路状态是RUNNING，如果VLAN内所有端口都不是RUNNING，则该VLAN接口的链路状态也不是RUNNING。

在VLAN接口上可以配置IP地址并指明与此接口相连的网段的网络前缀（可转换为网络掩码）。目前交换机只支持一个VLAN接口上配置一个IP地址。在配置IP地址之前用户需要先创建VLAN并把相关的端口加入到VLAN中。缺省情况下交换机存在VLAN1的接口，并且在此接口上设置了IP地址192.168.0.1/24，用户也可以修改VLAN1接口的IP地址。除VLAN1以外的其它VLAN的接口缺省没有设置IP地址。

配置VLAN接口的IP地址的命令如下表：

命令	描述	CLI模式
Ip address <ip-prefix>	在VLAN接口上设置IP地址。参数包括接口的IP地址和相连网段的网络前缀。如果该VLAN接口原来存在IP地址，先删除原来的IP地址，再设置指定的IP地址。参数的格式为A.B.C.D/M。	接口配置模式
no ip address [ip-prefix]	删除VLAN接口的IP地址。如果指定了参数，该参数必须与设置时给定的参数相同，否则此命令无效。参数的格式为A.B.C.D/M。	接口配置模式

查看VLAN接口的命令如下表：

命令	描述	CLI模式
show interface [if-name]	查看VLAN接口的信息，包括接口的IP地址，MAC地址，管理状态，链路状态等。参数是VLAN接口的接口名，如果没有指定参数，则查看所有的端口和VLAN接口的信息。	普通模式，特权模式
show running-config	查看系统的当前配置，可以查看到VLAN接口的配置。	特权模式

例子：

在VLAN3接口上配置子网193.1.1.0，子网前缀为24(也就是掩码255.255.255.0)，接口的IP地址为193.1.1.1，并且查看VLAN3接口的信息。命令如下：

```
switch(config)#interface vlan3
switch(config-vlan3)#ip address 193.1.1.1/24
switch(config-vlan3)#end
switch#show interface vlan3
```

12.2 配置 ARP

ARP（Address Resolution Protocol）协议是为IP 地址到对应的MAC地址提供映射的协议。当源端把以太网数据帧发送到位于同一VLAN内的目的端时，是根据48位的以太网MAC地址来确定目的地的，目的端根据数据包的目的MAC地址来决定是否需要接收此数据包。

假定两个相邻网段的主机A和B通过iSpirit 8806交换机进行通信，主机A在发送数据给主机B之前，首先向与主机A直接相连的交换机的接口发出ARP请求报文，得到ARP应答后发送数据包到该接口。交换机收到此数据包后首先向主机B广播一个ARP请求报文，从主机B处得到ARP响应报文后,再把数据包发送给主机B。

交换机上有一个ARP高速缓存，称为ARP表，存放直接相连的网络中的IP地址到MAC地址的映射记录。ARP表中每一项都有一个生存时间，缺省是20分钟，当交换机在生存期间内没有收到该IP地址的ARP请求或应答报文，则该IP地址对应的ARP表项将被删除。

本节包括以下内容：

- 配置静态ARP
- 配置ARP绑定
- 查看ARP的信息

12.2.1 配置静态 ARP

在ARP表中存在两种不同的ARP表项，一种是静态ARP，一种是动态ARP。静态ARP是用户通过命令配置的ARP表项，系统不会自动刷新和删除，需要用户手工完成。动态ARP是系统根据收到的ARP请求或应答包自动学习到的ARP，系统自动创建和删除，实时更新和维护，不需要用户干预，但用户可以手工删除动态ARP表项。

交换机缺省没有配置静态ARP表项。需要注意的是当某个VLAN接口被删除或接口的子网网段IP改变时，原来的子网网段内的静态和动态ARP表项都被删除。

配置静态ARP的命令如下表：

命令	描述	CLI模式
arp <ip-address> <mac-address> [if-name]	配置静态ARP表项。第一个参数是IP地址，IP地址必须在某个子网网段内。第二个参数是MAC地址，MAC地址必须是单播MAC地址，MAC地址的格式为HHHH.HHHH.HHHH，如0010.5cb1.7825。第三个参数是二层接口名称，可选，表示静态arp表项关联到特定二层接口。	全局配置模式

no arp {<ip-address> | <ip-prefix> | all | dynamic | static | dhcp-relay}	删除ARP表项。包括删除一个IP的ARP表项；删除一个网段的ARP表项；删除所有的ARP表项；删除所有的动态ARP表项；删除所有的静态ARP表项；删除所有的DHCP relay学习到的ARP表项。	全局配置模式

12.2.2 配置 ARP 绑定

ARP绑定是为了增强网络的安全性考虑的。对于某个子网网段，只允许规定的IP地址和其对应的MAC地址的主机可以访问网络，防止非法用户使用网络。当某个接口的子网网段做了ARP绑定后，该接口不学习动态ARP表项，该接口的所有ARP表项都是静态的，所有的ARP数据包都是根据静态ARP表项来处理的。

配置ARP绑定有下面几种方法：

第一种方法：先配置接口子网网段内的静态ARP表项，再给接口子网网段上锁。

第二种方法：先给接口子网网段上锁，再配置接口子网网段内的静态ARP表项。

第三种方法：先把接口子网网段内的所有动态ARP表项修改为静态ARP表项，再给接口子网网段上锁。这种方法对于用户来说使用非常方便。

接口子网网段缺省没有配置ARP绑定。

配置ARP绑定的相关命令如下表：

命令	描述	CLI模式
arp static {<ip-prefix> | all}	把某个网段内的或所有的动态ARP表项修改为静态ARP表项。	全局配置模式
arp lock <ip-prefix>	给某个网段上锁，上锁后该网段不再学习动态ARP表项，并且删除以前学习到的该网段内的所有动态ARP表项。	全局配置模式
arp unlock {<ip-prefix> | all}	给某个或所有的已经上锁的	全局配置模式

	网段解锁，解锁后网段可以学习动态ARP表项。	

例子：

对网段193.1.1.0/24进行ARP绑定，只允许IP地址为193.1.1.100，MAC地址为0010.5cb1.7825的主机和IP地址为193.1.1.101，MAC地址为0010.5cb1.7826的主机访问网络。

如果在配置ARP绑定时在ARP表中不存在IP地址为193.1.1.100和193.1.1.101的ARP表项，配置如下：

```
Switch(config)#arp lock 193.1.1.0/24
Switch(config)#arp 193.1.1.100 0010.5cb1.7825
Switch(config)#arp 193.1.1.101 0010.5cb1.7826
```

如果在配置ARP绑定时在ARP表中存在IP地址为193.1.1.100和193.1.1.101的ARP表项，配置如下：

```
Switch(config)#arp static 193.1.1.0/24
Switch(config)#arp lock 193.1.1.0/24
```

12.2.3 查看 ARP 的信息

查看ARP的信息的命令如下表：

命令	描述	CLI模式
show arp [<ip-prefix> | dynamic | static]	查看ARP表中的ARP表项信息，包括所有的ARP表项，某个网段的ARP表项，动态ARP表项和静态ARP表项。	普通模式，特权模式
show arp lock	查看ARP绑定的信息。	普通模式，特权模式
show running-config	查看系统的当前配置，可以查看到ARP的配置。	特权模式

12.3 配置静态路由

静态路由是由用户定义的、一条可使数据包从源地址通过指定路径到达目的地址的路由。当动态路由协议未能创建一条到特定目的的路由时，静态路由就显得特别重要。还可以通过配置某一静态路由为缺省路由，把无法确定路由的数据包发送到默认的网关。

静态路由是由管理员手工配置而成。适用于组网结构较简单的网络，管理员只需配置静态路由就能使交换机正常工作。静态路由由于不会有路由更新而不会占用宝贵的网络带宽。

缺省路由也是一种静态路由。简单地说，缺省路由就是在没有找到任何匹配的路由项情况下，才使用的路由。即只有当无任何合适的路由时，缺省路由才被使用。在路由表中，缺省路由以到网络0.0.0.0/0 （掩码为0.0.0.0） 的路由形式出现。若报文的目的地不在路由表中且路由表中也无缺省路由存在，该报文被丢弃的同时将返回源端一个ICMP 报文指出该目的地址或网络不可达信息。缺省路由在网络中是非常有用的。在一个包含上百个交换机的典型网络中，运行动态路由选择协议可能会耗费较大量的带宽资源，使用缺省路由就可节约因路由选择所占用的时间与包转发所占用的带宽资源，这样就能在一定程度上满足大量用户同时进行通信的需求。

交换机可以配置多条到同一目的地的静态路由，但只有其中的一条路由被激活，用于实际的数据转发。交换机缺省没有配置静态路由。

配置静态路由的命令如下表：

命令	描述	CLI模式
ip route <ip-prefix> <nexthop-address> [distance]	设置静态路由。第一个参数指定网段IP和网络前缀长度，第二个参数指定下一跳IP地址，第三个参数指定路由的管理距离。管理距离的范围从1到254，如果没有输入第三个参数，管理距离缺省为1。	全局配置模式
ip route <ip-address> <mask-address> <nexthop-address> [distance]	功能与上一个命令相同。第一个参数指定网段的IP地址，第二个参数指定网段的掩码，第三个参数指定下一跳IP地址，第四个参数指定路由的管理距离。管理距离的范围从1到254，如果没有输入第三个参数，	全局配置模式

	管理距离缺省为1。	
no ip route <ip-prefix> [nexthop-address]	删除静态路由。第一个参数指定网段IP和网络前缀长度，第二个参数指定下一跳IP地址。如果没有第二个参数，则删除与指定网段匹配的所有路由。如果有第二个参数，则删除与指定网段和下一跳都匹配的路由。	全局配置模式
no ip route <ip-address> <mask-address> [nexthop-address]	功能与上一个命令相同。第一个参数指定网段的IP地址，第二个参数指定网段的掩码，第三个参数指定下一跳IP地址。如果没有第三个参数，则删除与指定网段匹配的所有路由。如果有第三个参数，则删除与指定网段和下一跳都匹配的路由。	全局配置模式

查看路由的命令如下表：

命令	描述	CLI模式
show ip route [<ip-address> | <ip-prefix> | connected | static | rip | ospf]	查看激活的路由的信息，可选择查看所有的路由，某个路由，某个网段的路由，直接相连的路由、静态路由、RIP路由和OSPF路由。	普通模式，特权模式
show ip route database [connected | static | rip | ospf]	查看所有的路由的信息（包括激活的和未激活的路由），可选择查看所有的路由，直接相连的路由、静态路由、RIP路	普通模式，特权模式

	由和OSPF路由。	
show running-config	查看系统的当前配置，可以查看到静态路由的配置。	特权模式

例子：

设置目的IP地址为200.1.1.0，子网掩码为255.255.255.0，下一跳为10.1.1.2，管理距离为1的静态路由。配置命令为：

Switch(config)#ip route 200.1.1.0 255.255.255.0 10.1.1.2

或 Switch(config)#ip route 200.1.1.0/24 10.1.1.2

删除目的IP地址为200.1.1.0，子网掩码为255.255.255.0，下一跳为10.1.1.2 的静态路由。配置命令为：

Switch(config)#no ip route 200.1.1.0/24

或 Switch(config)#no ip route 2001.1.0/24 10.1.1.2

或 Switch(config)#no ip route 200.1.1.0 255.255.255.0

或 Switch(config)#no ip route 200.1.1.0 255.255.255.0 10.1.1.2

12.4 路由冗余备份

在实际的网络中，一个数据包到达目的地可能存在着多条路径，因此在交换机的路由表中存在同一目的地的多条路由。在这些同一目的地的多条路由中，交换机会激活一条最优路径的路由，这条路由用于数据包的转发，这样数据包可以以最优的路径到达目的地。当这条最优的路径出现故障时，交换机会从剩下的同一目的地的路由中激活一条最优路径的路由，以此类推，交换机就实现了同一目的地的路由的冗余备份功能。

路由是否被激活有两个先决条件，只有满足了这两个先决条件的路由才有可能被激活，如果不满足这两个先决条件的路由不可能被激活。路由激活的两个先决条件如下：

1、 路由的下一跳IP地址所在的子网接口是LINK UP的。

2、 路由的下一跳IP地址是可达的，也就是说交换机有下一跳IP地址的ARP条目。

对于同一目的地只有一条路由满足上面的先决条件的情况，则该路由被激活，对于同一目的地有多条路由满足上面的先决条件的情况，则从这些路由中选择一条最优路由被激活，而其它的路由不被激活。

在同一目的地的多条路由中，可以是静态路由和动态路由（RIP、OSPF等协议学习到的路由），静态路由和动态路由可以是多条。每一条路由都有一个管理距离，管理距离是选择最优路由的一个非常重要的因素，管理距离越小，路由的优先级越高。每一种类型的路由都有一个缺省的管理距离，管理距离可以通过配置命令修改。每一类路由的缺省管理距离如下表：

路由类型	缺省管理距离
直连子网路由	0
静态路由	1
RIP路由	120
OSPF路由	110

缺省情况下，路由的优先级从高到低的顺序为：直连子网路由、静态路由、OSPF路由、RIP路由。其中，静态路由，OSPF路由和RIP路由的管理距离都可以修改，管理员可以根据网络的情况灵活调整各种路由类型的管理距离。

对于同一目的地的多条满足路由激活先决条件的路由，从中选择一条激活的路由的规则如下：

1、 选择管理距离最小的路由作为最优路由，如果这样的路由只有一条，则该路由被激活。

2、 如果管理距离最小的路由有多条，并且路由的类型不同（如一条是静态路由，另一条是OSPF路由），则按路由加入到路由表的顺序来选择，后加入的一条路由被激活。

3、 如果管理距离最小的路由有多条，并且路由的类型相同（如两条路由都是静态路由），则按路由的下一跳IP地址的大小来选择，下一跳IP地址小的路由被激活。

当发生下列情况时，同一目的地的路由需要重新选择激活的路由，也就是发生路由切换：

1、 被激活的路由的下一跳IP地址所在的子网接口LINK DOWN。

2、 被激活的路由的下一跳IP地址不可达。

3、 加入了或学习到一条满足路由激活先决条件的比现在激活的路由更优的路由。

4、 被激活的路由被删除。

下面是一个同一目的地的路由选择激活路由的例子，假设表中的路由都满足路由激活的先决条件，根据选择激活路由的规则，下一跳IP地址为192.168.0.100的静态路由被激活。

网络前缀	下一跳IP	路由类型	管理距离	是否被激活
10.1.1.0/24	192.168.0.100	静态路由	1	Y
10.1.1.0/24	192.168.0.101	静态路由	1	N
10.1.1.0/24	192.168.1.100	RIP路由	120	N
10.1.1.0/24	192.168.2.100	OSPF路由	110	N

12.5 配置策略路由

一般情况下，数据包在做三层转发时是通过查找三层设备的路由表来决定输出接口和下一跳IP地址的。目前交换机只支持一条激活的路由，也就是说同一目的地的数据包只能选择一条路径。在内部网多出口的应用中，用户想根据指定的策略来决定数据包的输出接口和下一跳IP地址，交换机的路由表中的路由和路由冗余备份功能满足不了这种应用要求。为此，交换机实现了策略路由功能来满足这种应用要求，策略路由比路由表中的路由的优先级高，数据包三层转发时先匹配策略路由，如果匹配不到策略路由，才使用路由表中的路由来做三层转发。

目前交换机只实现了部分策略路由功能，在应用上有一定的局限性，主要有以下几个方面：

1、 只实现了基于输入VLAN接口的策略路由，用户可以根据数据包输入接口的VLAN来选择出口的下一跳IP地址。

2、 数据包在查找路由表时只有匹配到缺省路由（路由0.0.0.0/0）时才能使用策略路由。如果数据包匹配策略路由（满足条件1），但在查找路由表时没有匹配到缺省路由，而是匹配到其它的路由时，不使用策略路由，还是使用路由表中查找到的路由进行三层转发。

3、 交换机的10G2X模块不支持策略路由，如果数据包从10G2X模块输入，即使匹配到策略路由（满足条件1和2），也不会使用策略路由，而是使用路由表中查找到的缺省路由。

管理员配置了策略路由，但策略路由还不一定能够生效，策略路由生效有一定的条件，只有生效的策略路由才会用于实际的三层转发。策略路由必须满足下面的所有条件才能生效：

1、策略路由中指定的输入VLAN必须存在并且该VLAN接口上配置了IP地址。

2、策略路由中指定的下一跳IP地址必须是某一个缺省路由的下一跳IP地址。

3、 策略路由中指定的下一跳IP地址所在的子网接口必须是LINK UP。

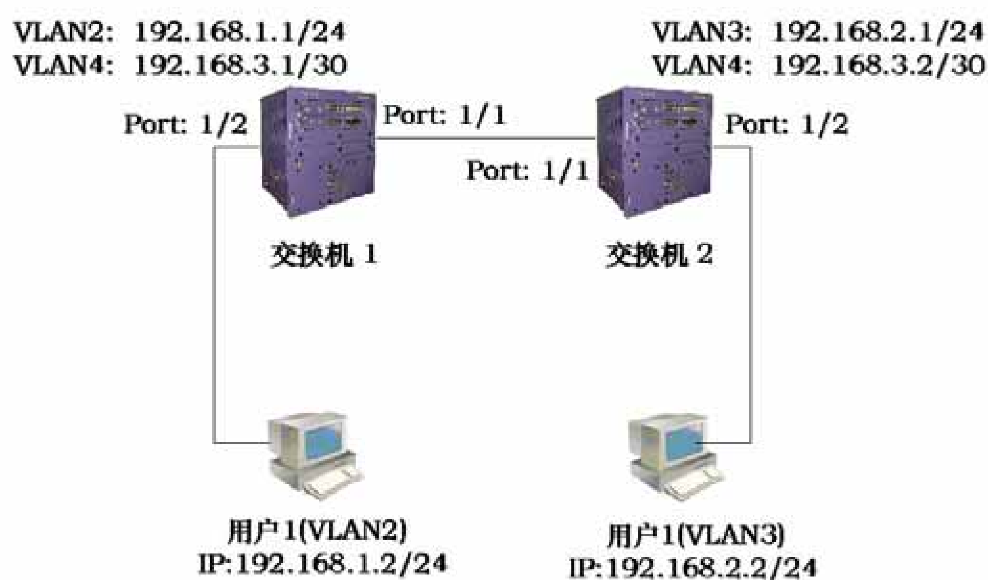
4、 策略路由中指定的下一跳IP地址必须是可达的，也就是交换机上有该下一跳IP地址的ARP表项。

策略路由可以实现路由的负载分担功能，当策略路由生效时，匹配策略路由的数据包使用策略路由进行三层转发，当策略路由失效时，数据包还可以使用激活的缺省路由进行三层转发。

交换机缺省没有配置策略路由，配置和显示策略路由的命令如下表：

命令	描述	CLI模式
policy route <vlan-id> <nexthop-address>	设置一条策略路由。第一个参数指定输入接口的VLAN号，范围从1到4094。第二个参数指定策略路由的下一跳IP地址。	全局配置模式
no policy route <vlan-id>	清除一条策略路由。参数是输入接口的VLAN号，范围从1到4094。	全局配置模式
show policy route	显示所有的策略路由。	普通模式，特权模式
show running-config	查看系统的当前配置，可以查看到策略路由的配置。	特权模式

12.6 IP 路由配置示例



12.6.1 三层接口

在交换机1上配置VLAN2对应的三层接口，同时分配一个IP地址192.168.1.1/24。

配置如下：

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switch access vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
```

验证：用户1能够ping通交换机1的VLAN2对应的三层接口IP地址。

12.6.2 静态路由

要求通过配置静态路由，使两个用户PC之间能够互通。

交换机1上配置如下：

Switch#config t
Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

交换机2上配置如下：

Switch#config t
Switch(config)#ip route 192.168.1.0/24 192.168.3.1

验证：用户1能ping通用户2，用户2能ping通用户1。

12.6.3 ARP

把交换机1的VLAN2进行ARP锁定，配置用户1的静态ARP，只允许用户1从VLAN2接入。假定用户1的MAC地址是00:00:00:00:00:01。

交换机1配置如下：

Switch#config t
Switch(config)#arp lock 192.168.1.0/24
Switch(config)#arp 192.168.1.2 0000.0000.0001

验证：用户1能够ping通交换机1的VLAN2对应的三层接口IP地址。如果把用户1的IP地址改成192.168.1.3，则ping不通交换机1的VLAN2的接口IP地址。

第13章 配置RIP

本章主要包括以下内容：

- RIP 介绍
- RIP 配置
- RIP 配置示例

13.1 RIP 介绍

RIP（路由信息协议 Routing Information Protocol）是较早开发的动态路由协议，使用距离向量算法，多应用在小型网络中。RIP协议报文封装在UDP报文中，使用UDP端口520。RIP的主要思想是使用跳数（hop）来衡量到达宿主机的距离，每经过一台路由器跳数增加1，以此来计算路由的权值（metric），进行选路。RIP约定最大跳数为15，跳数16标记为网络不可达。RIP使用广播整个路由表的方式让网络的中的路由器同步路由信息，每隔30秒定时更新一次报文，若某条路由条目在180秒内未收到从邻居发来的更新报文，则将其标记为不可达，如果再过120秒还未接收到有效更新，则将该路由删除。

RIP因其简单的思想容易实现，但也带来了相应的路由环路问题，为防止路由环，RIP引入了水平分割机制来规避路由器之间的欺骗。水平分割也即路由更新不会从接收到的接口发布出去。带毒性反转的水平分割是将路由更新从接收到的接口发布出去，但权值标记为不可达，这样能让邻居路由器快速识别环路而无需等待权值增加到不可达。

路由表中的路由条目应包含目的地址（主机或网络）下一跳地址、转发接口、路由权值、计时器（当接收到路由更新时计时器被重置）路由标记。

RIP启动时，立即以广播（RIP-1）或组播（RIP-2）形式发送一全表请求报文，相邻路由器接收到请求报文就会将自己完整的路由表以响应报文回送。路由器接收到响应报文会逐条处理路由，并修改自己的路由表，当有新路由时会立即产生一触发更新报文。经过一连串的更新过程，最终RIP收敛，网络中各个路由器均保持了最新的一致的路由信息。网络稳定后，RIP依然每隔30秒向邻居广播本地路由表，各个路由器根据接收到的路由更新报文维护自身的路由信息，进行最优选路。RIP使用超时机制处理久未更新的路由条目，以保证路由的实时正确。

RIP多应用于校园网及结构简单的较连续的区域性网络，复杂的大型网络RIP难以胜任。

13.2 RIP 配置

启动RIP协议后可进行RIP各功能各属性的配置。RIP的配置多在RIP配置模式和接口配置模式下。

RIP的配置包括：

- 启动 RIP 并进入 RIP 配置模式

- 使能 RIP 接口
- 配置单播报文传送
- 配置接口的工作状态
- 配置缺省路由权值
- 配置管理距离
- 配置计时器
- 配置版本
- 引入外部路由
- 配置路由过滤
- 配置附加路由权值
- 配置接口的 RIP 版本
- 配置接口的收发状态
- 配置水平分割
- 报文认证
- 配置接口权值

13.2.1 启动 RIP 并进入 RIP 配置模式

模式：全局配置模式

命令：router rip

启动rip并进入rip配置模式

命令：no router rip

关闭rip协议

缺省：不运行rip协议

13.2.2 使能 RIP 接口

RIP工作时可指定某些接口，将其所在的网络配置成RIP网络，即可在其上收发RIP协议报文。

模式：RIP配置模式

命令：network <network-address>

使能rip接口

命令：no network <network-address>

关闭rip接口

参数：有A.B.C.D/M和A.B.C.D A.B.C.D两种形式，前一种指定网络ip及掩码长度，后一种指定网络ip及掩码。

缺省：RIP协议启动后在所有接口禁用

RIP协议启动后必须指定其工作的网段，RIP只能在指定网段的接口上运行，对于那些不在指定网段的接口，RIP既不接收发送路由也不会将接口路由转发。在RIP的视图中，那些不在指定网段的接口不存在。参数network-address为使能或者不使能的网络地址，可配置为接口ip地址。network命令使能该地址的网段的接口。例如：有一接口的ip地址为192.160.1.1，使用命令network 192.160.1.1/24，使用show running-config命令看到的是network 192.160.1.0/24。

13.2.3 配置单播报文传送

RIP协议版本1使用广播交换报文，版本2使用组播（224.0.0.9）交换报文，当在不支持广播的链路上运行RIP协议时，需要指定特定的单播地址来交换报文。

模式：RIP配置模式

命令：neighbor <ip-address>

配置对端单播ip地址

命令：no neighbor <ip-address>

取消对端单播ip地址的设置

参数：ip-address为指定的单播ip地址

缺省：RIP协议不向任何单播地址发送报文

13.2.4 配置接口的工作状态

RIP协议运行在某些网络中，可能仅需要RIP接口路由，并不希望在该接口上广播RIP路由。使用network命令可指定该接口上收发RIP协议报文，且可以获知该接口路由。使用

passive-interface命令仅获知该接口路由而阻塞该接口的广播。

模式：RIP配置模式

命令：passive-interface <if-name>

配置接口为被动状态

命令：no passive-interface <if-name>

取消接口被动状态

参数：if-name为约定的三层接口名（例如：vlan1 vlan2 …）

缺省：使能的RIP接口均不为passive状态

13.2.5 配置缺省路由权值

在引入外部路由时，需要指定一个路由权值；当未指定其路由权值时，使用这个缺省路由权值。

模式：RIP配置模式

命令：default-metric <metric>

设置引入外部路由时缺省路由权值

命令：no default-metric [metric]

恢复引入外部路由时缺省路由权值为默认值1

参数：metric取值在1~16之间，大于1，小于16。

缺省：metric值为1，使用no default-metric命令恢复到缺省值。

13.2.6 配置管理距离

每一种协议都有约定的优先级，管理距离即使用路由策略时选择路由的优先级。当存在到达同一目的地的两条相同路由（来自不同的路由协议），则管理距离越小，优先选择该协议的路由。

模式：RIP配置模式

命令：distance <distance>

设置管理距离值

命令：no distance [distance]

恢复管理距离为缺省值

参数：distance取值在1~255之间

缺省：distance值为120，使用no distance命令恢复到缺省值。

13.2.7 配置计时器

RIP协议有三个计时器，其一是完整路由表每30秒向所有RIP接口广播一次，其二是RIP路由表中每条路由若180秒未接收到更新则标记metric为16，其三是RIP路由表中每条路由若标记metric为16后又120秒未被有效更新则从路由表中删除。

模式：RIP配置模式

命令：timers basic <update> <timeout> <garbage>

设置三个计时器值

命令：no timers basic

恢复计时器为缺省值

参数：第一个参数update为整个RIP路由表定时更新计时器，第二个参数timeout为每条路由超时未更新计时器，第三个参数garbage为每条路由标记为无效后超时需删除计时器；三个计时器的取值范围均为5~(2^{31}-1)。

缺省：update为30秒更新一次；timeout为180秒标记为无效；garbage为120秒删除。

13.2.8 配置版本

RIP协议目前有版本1（RFC1058）和版本2（RFC2453），配置的版本值会体现在协议报文的版本域中。

模式：RIP配置模式

命令：version <version>

设置RIP协议为版本1或者版本2

命令：no version [version]

恢复RIP协议版本为缺省值

参数：version可取值1或者2

缺省：版本2

13.2.9 引入外部路由

RIP允许用户将其他协议的路由信息引入到RIP的路由表中，RIP可引入的路由协议（类型）包括：connected、static、OSPF、IS-IS、BGP。

模式：RIP配置模式

命令：redistribute {kernel | connected | static | ospf | isis | bgp} [metric <metric> | route-map <route-map-name>]

引入其他协议路由

命令：no redistribute {kernel | connected | static | ospf | isis | bgp} [metric <metric> | route-map <route-map-name>]取消引入的路由

参数：第一个参数为引入其他协议的名称，可引入的有直连、静态、ospf、is-is、bgp；第二个参数为引入时设置的权值，取值1~16之间；第三个参数为引用的route-map名称，route-map在全局配置模式下配置，可参看命令手册。

缺省：RIP协议不引入任何外部协议

13.2.10 配置路由过滤

RIP提供路由过滤功能，通过指定的访问控制列表和地址前缀列表，对接收到的路由和发布的路由，配置策略规则进行过滤。

模式：RIP配置模式

命令：distribute-list <acl-name> {in | out} [if-name]

使用access-list过滤接口的输入输出

命令：no distribute-list <acl-name> {in | out} [if-name]

取消使用access-list过滤

参数：acl-name表示引用的access-list的名；if-name表示应用到的RIP接口；in和out

表示应用在接收到路由的方向还是发布路由的方向上。

命令：distribute-list prefix <pre-name> {in | out} [if-name]

使用prefix-list过滤

命令：no distribute-list prefix <pre-name> {in | out} [if-name]

取消使用prefix-list过滤

参数：pre-name表示引用的prefix-list的名；if-name表示应用到的RIP接口；in和out表示应用在接收到路由的方向还是发布路由的方向上。

缺省：RIP协议不对任何接收和发送的路由进行过滤

access-list和prefix-list在全局配置模式下配置，可参考命令手册。

13.2.11 配置附加路由权值

附加路由权值是对RIP协议的路由权值在输入输出时添加的一个偏移量值，并不直接改变路由表中路由的权值，而是在接口接收发送路由时增加一个偏移量。

模式：RIP配置模式

命令：offset-list <acl-name> {in | out} <offset> [if-name]

使用access-list对接口输入输出路由的权值增加一偏移量

命令：no offset-list <acl-name> {in | out} <offset> [if-name]

取消输入输出路由的权值的偏移量

参数：acl-name表示引用的access-list名；in和out表示应用在输入还是输出方向上；offset表示偏移量的值，取值0~16之间；if-name表示应用到的RIP接口。

缺省：在接收报文时每条路由的附加权值为1，在发送报文时每条路由的附加权值为0。

13.2.12 配置接口的 RIP 版本

RIP分RIP-1和RIP-2两个版本，可以对使能的RIP协议的接口指定其处理的RIP报文版本。接收方向，可区分为仅接收RIP-1的报文，仅接收RIP-2的报文，既接收RIP-1又接收RIP-2的报文。在发送方向上，可区分为发送RIP-1的报文，发送RIP-2的报文（以广播方式），发送RIP-2的报文（以组播方式），既发送RIP-1又发送RIP-2的报文。RIP-2有广播和组播两种发送报文方式，使用组播既可以避免同一网络中没有运行RIP的主机不接收RIP的广播报文，又可以避免运行RIP-1的主机错误的处理RIP-2的带有子网掩码的路由。

模式：接口配置模式

命令：ip rip receive version {1 | 2}

设置接口仅接收版本1的报文或者仅接收版本2的报文

参数：版本1或者版本2

命令：ip rip receive version {1 2 | 2 1}

设置接口既可以接收版本1的报文又可以接收版本2的报文

参数：可以写作1 2或者2 1

命令：no ip rip receive version [1 | 2 | 1 2 | 2 1]

恢复接口接收报文设置为缺省值

缺省：版本2组播方式

命令：ip rip send version {1 | 2 | 1-compatible}

设置接口仅发送版本1的报文或者仅发送版本2的报文

参数：版本1或者版本2；1-compatible表示版本2的接口发送出兼容版本1的报文，也即广播报文而非组播。

命令：ip rip send version {1 2 | 2 1}

设置接口既可以发送版本1的报文又可以发送版本2的报文

参数：可以写作1 2或者2 1

命令：no ip rip send version [1 | 2 | 1-compatible | 1 2 | 2 1]

恢复接口发送报文设置为缺省值

缺省：版本2组播方式

13.2.13 配置接口的收发状态

在RIP模式下使用network命令使能了RIP接口后，还可以在接口模式下指定其收发协议报文的状态，是否接收协议报文或者是否发送协议报文。

模式：接口配置模式

命令：ip rip receive-packet

配置接口接收协议报文

命令：no ip rip receive-packet

配置接口不接收协议报文

命令：ip rip send-packet

配置接口发送协议报文

命令：no ip rip send-packet

配置接口不发送协议报文

缺省：使能接收发送协议报文

注意区别，network命令启动某一网络运行RIP协议，在该网络内的接口收发协议报文，该接口路由包含在路由表中。passive-interface命令是在network命令生效后，使该接口不收发协议报文，但该接口路由仍包含在路由表中。ip rip receive-packet和ip rip send-packet命令也是在network命令生效后，具体指定接口是否接收或者是否发送协议报文。

13.2.14 配置水平分割

水平分割是指从本接口接收到的路由不从本接口发出。带毒性反转的水平分割是指从本接口接收到的路由依然从本接口发出，但其metric值标记为16。水平分割可以在一定程度上避免产生环路，带毒性反转的水平分割比普通水平分割效率更高，直接标记不可达。但在NBMA网络上需要禁止水平分割来获取正确的路由。

模式：接口配置模式

命令：ip rip split-horizon [poisoned]

启动接口水平分割功能或带毒性反转的

命令：no ip rip split-horizon

禁止接口的水平分割功能

参数：无poisoned参数表示启动普通水平分割功能，带poisoned参数表示启动带毒性反转的水平分割功能。

缺省：带毒性反转的水平分割

13.2.15 报文认证

RIP-1不支持报文认证，RIP-2支持报文认证，有两种认证方式，明文认证和MD5认证。明文认证中未加密的认证数据随报文一同传送，不能提供安全保障，不能应用于安全性要求

较高的网络。密码的设置分普通密钥及密钥链两种，普通密钥保存独立的字符串，密钥链管理密钥的id、内容、接收的生存期、发送的生存期。密钥链管理详见命令参考手册。

模式：接口配置模式

命令：ip rip authentication mode {text | md5}

设置认证模式明文或者md5

命令：no ip rip authentication mode [text | md5]

取消认证

参数：text为明文认证，md5认证。

缺省：无认证

命令：ip rip authentication string <password>

设置认证的密码串

命令：no ip rip authentication string [password]

取消认证的密码串

参数：16个字节的认证密码

命令：ip rip authentication key-chain <key-chain-name>

设置认证的key-chain

命令：no ip rip authentication key-chain [key-chain-name]取消认证的key-chain

参数：引用的key-chain的名；key-chain在全局配置模式下配置，参看命令手册。

13.2.16 配置接口权值

模式：接口配置模式

命令：ip rip metric <metric>

配置接口权值

命令：no ip rip metric

恢复接口权值为默认值

参数：metric取值1-16之间，表示该接口学习到的路由条目需增加的权值。

缺省：为1

13.2.17 显示信息

模式：普通模式或特权模式

命令：show ip protocols

显示所有运行中的协议的信息

命令：show ip protocols rip

显示RIP协议信息

命令：show ip rip

显示RIP路由

命令：show ip rip database

显示RIP数据库

命令：show ip rip database count

显示RIP数据库条目数

命令：show ip rip interface [if-name]

显示RIP接口信息

参数：if-name为约定的三层接口名

模式：特权模式

命令：show running-config

显示交换机当前配置，包括RIP配置。

命令：show running-config rip

显示RIP协议的当前配置。

13.3 RIP 配置示例

(1) 配置

三台交换机两两相连，分别有6 个网段，都启用rip 协议，实现三台PC 机之间能够两两互通。

在交换机1上：

```
Switch# configure terminal
Switch(config)#router rip
Switch(config-rip)#network 192.168.1.0/24
Switch(config-rip)#network 10.1.1.0/24
Switch(config-rip)#network 10.1.2.0/24
```

在交换机2上：

Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.2.0/24

Switch(config-rip)#network 10.1.2.0/24

Switch(config-rip)#network 10.1.3.0/24

在交换机3上：

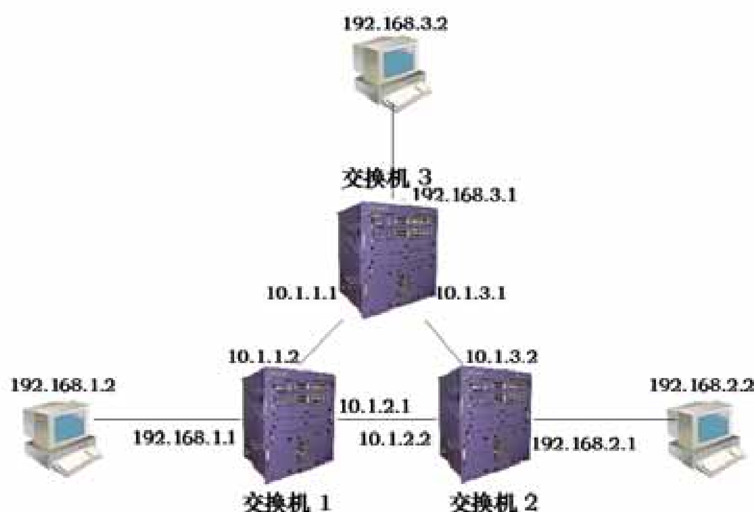
Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.3.0/24

Switch(config-rip)#network 10.1.1.0/24

Switch(config-rip)#network 10.1.3.0/24



(2) 验证

使用下面的命令查看RIP的信息：

show ip protocols rip

show ip rip database

show ip rip interface

第14章 配置OSPF

本章主要包括以下内容：

- OSPF 介绍
- OSPF 配置
- OSPF 配置示例

14.1 OSPF 介绍

OSPF（开放最短路径优先协议 Open Shortest Path First）是基于链路状态算法的协议，可支持较大规模网络，收敛速度较快。

运行 OSPF 协议的路由器各自维护链路状态数据库（LSDB），该数据库描述整个自治系统的拓扑结构，仿佛一张地图。当所有路由器的数据库同步后，每台路由器以自身为视角，计算出到达自治系统中其他目的结点的最短路由，维护在自己的路由表中。当网络中拓扑发生变化时，路由器只需要将变化的链路状态封装在链路状态更新（LSU）报文中广播出去，所有的路由器会再次同步本地的数据库，重新计算路由。每台路由器将自己看到的链路状态广播（LSA）都发布出去，集中起来，就形成了整个网络的拓扑描述 LSDB，将其转换为带权的有向图，就可以使用 SPF 算法计算出路由表。

在广播网络中每台路由器都需要将各自的状态信息广播到其他路由器，就会建立多个两两邻接关系，这会带来大量没有必要的报文传送。为此，OSPF 约定了指定路由器（DR）和备份指定路由器（BDR），路由器将链路信息发给 DR，由 DR 收集整理再发给所有的路由器。有效的减少了广播网络上路由器之间的邻接数量。

OSPF 支持五种协议报文：

HELLO 报文，周期性的广播给邻居，用于发现和维护邻居，进行 DR 选举，包含一些接口属性值，HELLO 报文中的一些参数必须一致方能建立邻居。

DD 报文（Database Description）在同步过程中使用 DD 报文来描述自己的 LSDB，包括每一条 LSA 的 head，通过 LSA head 可以唯一确定一条 LSA，对端路由器可以判断自己是否有这条 LSA；若无，再请求完整的 LSA。

LSR 报文（Link State Request）两台路由器交换 DD 报文之后，就会知道对端路由器有哪些 LSA 是本地缺少的，这时需要发送 LSR 报文请求完整的 LSA。请求时只需要 LSA head 即可。

LSU 报文（Link State Update）是多条 LSA 的集合。

LSAck 报文（Link State Acknowledgement）是对接收到的 LSU 报文确认，保证可靠的传递链路信息。使用 LSA head 确认。

Router-id 概念：自治系统内路由器的唯一标识。

区域（area）：OSPF 若运行在一个较大的网络中，由于路由器数量的大增，会导致 LSDB 非常庞大，并使同步的时间及计算路由的时间增加，占用大量存储空间及 CPU 资源。并且越大的网络，拓扑变化越频繁，使得网络经常处于变动中，路由器需要花费大量的时间传递报文计算路由，无谓的占用了网络带宽。因此 OSPF 引入区域概念，将路由器划分在不同

的区域内，LSDB 只在区域内同步并在区域内计算路由，区域之间的路由交互由边界路由器（ABR）来完成。这样在区域内路由器数量会有所限制，LSDB 也会局限于较小的容量，计算路由的时间会大大缩减，当拓扑变化时收敛也很快。区域概念有效的将一个大范围的网络进行分组，在各个区域内部承担小范围的路由功能。区域之间的路由在骨干区域上交互（区域 ID 为 0 的区域）。因此所有非骨干区域必须与骨干区域相连，也即 ABR 至少有一个接口连接骨干区域。若网络规划，有非骨干区域无法与骨干区域连通，则必须配置虚链路建立逻辑上的通路，也即骨干区域上的某一 ABR 与非骨干区域的某一 ABR 通过一传输区域建立点到点的链路。那么骨干区域上的域间路由信息也会通过虚链路发布到该非骨干区域。

14.2 OSPF 配置

OSPF 协议启动后进入 OSPF 配置模式可进行相应属性及功能设置。OSPF 配置命令多在 OSPF 配置模式下及接口配置模式下。

OSPF 的配置包括：

- 启动 OSPF 并进入 OSPF 模式
- 使能接口
- 指定主机
- 配置路由器 ID
- 配置邻接点
- 禁止接口发送报文
- 配置 SPF 计时器
- 配置管理距离
- 引入外部路由
- 配置接口的网络类型
- 配置 hello 报文发送时间间隔
- 配置邻居路由器失效时间
- 配置重传间隔
- 配置接口延时
- 配置接口在 DR 选举中的优先级
- 配置接口上发送报文的代价

- 配置接口发送 DD 报文是否填 MTU 值
- 配置接口报文认证
- 配置区域虚链路
- 配置区域路由聚合
- 配置区域报文认证
- 配置 stub 区域
- 配置 nssa 区域
- 配置外部路由聚合
- 配置外部路由的缺省权值

14.2.1 启动 OSPF 并进入 OSPF 模式

OSPF 协议可运行多个副本，使用进程号（process-id）来标识；启动 OSPF 协议时需说明启动的是哪个进程号的进程；若无参数则进程号为 0。

模式：全局配置模式
命令：router ospf [process-id]
启动进程号 process-id 的 OSPF 进程并进入其模式

命令：no router ospf [process-id]
关闭进程号 process-id 的 OSPF 进程

参数：process-id取值 1~(2^{16}-1)之间，表示启动的OSPF进程号；若不带参数process-id则启动进程号为 0 的OSPF。
缺省：不运行 OSPF 协议

14.2.2 使能接口

OSPF 协议的可贵之处在于引入了分层思想，将一个完整的自治系统分成不同的区域，以期建立一个概念上的层次化网络模型。区域是逻辑上的，将自治系统中的路由器人为的分组。当路由器的不同接口属于不同的区域时，也即跨区域时，称其为边界路由器 ABR。对

于每个启动 OSPF 协议的网段只能隶属于某一特定区域，也即路由器上每个运行 OSPF 协议的接口必须属于指定区域。区域使用区域号（area-id）来标识，区域号为 0 的区域为骨干区域。不同区域之间的路由信息通过边界路由器来传递。区别于 RIP 协议，在接口上运行 OSPF 协议时必须指定其所属区域。

模式：OSPF 配置模式

命令：network <network-address> area <area-id>

指定区域指定接口运行 OSPF 协议

命令：no network <network_address> area <area-id>

关闭特定区域特定接口上的 OSPF

参数：network-address有A.B.C.D/M和A.B.C.D A.B.C.D两种形式，前一种指定网络ip及掩码长度，后一种指定网络ip及掩码。area-id也有两种形式A.B.C.D和整型数，前一种使用点分十进制格式，后一种取值 0~(2^{32}-1)之间。

缺省：OSPF 协议启动后不使能接口

14.2.3 指定主机

模式：OSPF 配置模式

命令：host <ip-address> area <area-id> [cost <cost>]

配置主机路由

命令：no host <ip-address> area <area-id> [cost <cost>] 取消主机路由

参数：ip-address 使用 A.B.C.D 格式，表示某一区域内一指定主机，在路由器的链路表示上是 stub 类型。area-id 同 network 命令中说明。cost 表示指定该链路的代价，为可选参数。

缺省：cost 若不配置则缺省为 0

14.2.4 配置路由器 ID

路由器的 ID 是一个 32bit 的无符号整数，是一台路由器在自治系统中唯一的标识。路由器 ID 可以手工配置，配置时需保证自治系统内任意两台路由器的 ID 都不相同。若不配置，则路由器使用 loopback 接口的 IP 地址；若 loopback 无 IP 则从当前接口的 IP 地址中选择最高地址作为 ID。为了保证 OSPF 运行稳定，在网络规划时就应进行路由器 ID 的划分并手工配置。

模式：OSPF 配置模式

命令：ospf router-id <router-id>

配置路由器 ID

命令：no ospf router-id

取消路由器 ID

命令：router-id <router-id>

命令：no router-id [router-id]

参数：router-id 使用 A.B.C.D 格式

缺省：OSPF 协议启动后会根据规则自动生成路由器 ID。规则如下：首先选用该命令配置的 router-id；若无，选择 loopback 的 IP 地址；若无，选择当前接口的最高 IP 地址；若无，则为 0.0.0.0。

两组命令功能一样。

14.2.5 配置邻接点

OSPF 协议交互协议报文通过组播方式，使用组播地址 224.0.0.5 或者 224.0.0.6。当 OSPF 协议运行在不支持广播的链路上，例如 NBMA，则必须进行一些配置，使用单播方式交互协议报文。这时可手工指定对端的 IP 地址及相应属性值。

模式：OSPF 配置模式

命令：neighbor <ip-address> [priority <prio> | poll-interval <deadtime> | cost <cost>]

指定对端邻接点及设置属性

命令：no neighbor <ip-address> [priority <prio> | poll-interval <deadtime> | cost <cost>]取消对端邻接点及属性设置

参数：ip-address对端的IP地址，为A.B.C.D格式；prio为对端优先级，取值 0~255 之间；deadtime为认为对端down的计时，若计时终止则不再向对端发送hello报文，取值 1~(2^{16}-1)之间；cost为到对端链路的代价，取值 1~(2^{16}-1)之间。

缺省：priority 为 1（为 0 则不参与 DR 选举）；poll-interval 为 120 秒；cost 为 10。

14.2.6 禁止接口发送报文

当在一个简单的网络中，OSPF 协议的接口仅表示两台设备之间的一个网段，仅仅是为了传输数据，那么将该接口设置为 passive 状态，阻塞 hello 报文在其链路上广播，这不影响获知该接口路由。

模式：OSPF 配置模式

命令：passive-interface <if-name>

配置接口为被动状态

命令：no passive-interface <if-name>

取消接口被动状态

参数：if-name 为三层接口名（例如：vlan1 vlan2…）

缺省：OSPF 协议启动后使能的接口均不为 passive 状态

将运行 OSPF 协议的接口指定为 passive 状态，该接口的直连路由仍可以发布，但接口上的 OSPF 报文将被阻塞，接口也无法建立邻居关系。在某些组网情况下，可有效节约网络资源。

14.2.7 配置 SPF 计算时间

当 OSPF 的链路状态数据库 LSDB 发生改变时，需要重新计算最短路径。如果每次改变都立即计算最短路径，将占用大量的资源，并影响路由器的效率。通过配置 delay 和 hold 两个值来调节 SPF 计算的时间间隔，可以抑止网络频繁变化引起的过于频繁的 SPF 计算，从而避免集中在一个时间内占用大量的系统资源，影响路由器运行效率。

SPF 计算有一计时器，每次按照抑止时间启动下一次的计算。当计时器终止需启动 SPF

计算时，重新计算上一次 SPF 计算到这次的抑止时间，若已超过了配置的抑止时间，则使用配置的延时时间来启动该计时器。若尚未超过配置的抑止时间则使用配置的抑止时间来计算所需要的延时时间。若该延时时间小于配置的延时时间则使用配置的延时时间，否则直接使用计算出的延时时间启动 SPF 计算。

模式：OSPF 配置模式

命令：timers spf <delay> <hold>

配置 SPF 计算间隔的 delay 及 hold 值

命令：no timers spf

恢复为缺省值

参数：delay 表示计算 SPF 时需要延时的时间；hold 表示两次 SPF 计算之间需要抑止的时间。

缺省：delay 为 5s；hold 为 10 秒

14.2.8 配置管理距离

路由器上可同时运行多个路由协议，如何在多个路由协议学习的路由信息中选择，就需要使用管理距离。当不同的协议发现同一条路由时，管理距离小的，优先被选择。

模式：OSPF 配置模式

命令：distance <distance>

配置管理距离

命令：no distance <distance>

恢复管理距离为缺省值

命令：distance ospf {intra-area <distance> | inter-area <distance> | external <distance>}

配置不同类型的管理距离

命令：no distance ospf

恢复三种类型的管理距离为缺省值

参数：distance 均取值 1~255 之间；intra-area 表示域内路由的管理距离；inter-area 表示域间路由的管理距离；external 表示外部路由的管理距离。

缺省：OSPF 协议的管理距离为 110；域内路由、域间路由、外部路由的管理距离为 0。

14.2.9 引入外部路由

路由器上可运行多个动态路由协议，不同路由协议之间可共享路由信息。OSPF 把其他路由协议学习的路由看作自治系统外部的路由，由自治系统边界路由器 ASBR 引入。引入外部路由时可指定权值、权值类型等属性。

OSPF 的路由分四种类型，其一是域内路由，其二是域间路由，这两类路由均是自治系统内的；其三是 type-1 的外部路由，其四是 type-2 的外部路由，这两类路由描述的是到自治系统外的目的地的路由。type-1 的路由是来自其他 IGP 的路由，OSPF 认为其可信度比较高，且与自治系统内的路由权值具有可比性，所以这类外部路由的花费是路由器本身到 ASBR 的花费与 ASBR 到目的地的花费之和。type-2 的路由是来自其他 EGP 的路由，OSPF 认为其可信度不太高，且其花费远大于自治系统内的路由花费，不具可比性，所以这类外部路由的花费仅使用 ASBR 到目的地的花费，而忽略路由器本身到 ASBR 的花费。

模式：OSPF 配置模式

命令：redistribute {kernel | connected | static | rip | isis | bgp} [metric <metric> | metric-type <type> | route-map <route-map-name> | tag <tag>]

命令：no redistribute {kernel | connected | static | rip | isis | bgp} [metric <metric> | metric-type <type> | route-map <route-map-name> | tag <tag>]

参数：第一个必选参数为可引入的外部路由的类型，有直连、静态、RIP、IS-IS、BGP；第二个参数为引入外部路由时设置的权值，取值 0~(2^{24}-1)之间；第三个参数为引入的两类外部路由，分type-1 和type-2，type-1 为IGP路由，type-2 为EGP路由；第三个参数为引用的route-map的名，route-map在全局配置模式下配置，可参看命令手册；第四个参数为tag，取值 0~(2^{32}-1)之间，为外部路由属性。

缺省：不引入任何外部路由协议

14.2.10 配置接口的网络类型

OSPF 协议是以本身路由器为视角的，每台路由器均将自己邻接的网络拓扑描述出来，传递给其他路由器。OSPF 根据链路层协议类型将接口链路的网络类型分为四种：一是广播类型（链路层协议是 Ethernet、FDDI etc）；二是 NBMA 非广播多路访问类型（链路层协议是 FR、ATM、HDLC、X.25 etc）；三是点到多点类型，没有一种链路层协议会被缺省认为是点到多点类型。点到多点类型必须是由其他的网络类型强制配置的。最常见的做法是将非全连通的 NBMA 改为点到多点网络。四是点到点类型（链路层协议是 PPP、LAPB、POS）。

在没有多路访问能力的广播网络上，可将接口配置成 NBMA 类型。在 NBMA 网络中并非所有路由器之间都直接可达时，可将接口配置成点到多点类型。

OSPF 协议中约定的 NBMA 网络是全连通的，非广播的，多点可达的。点到多点网络不一定是全连通的。NBMA 需要进行 DR 选择，点到多点网络中没有 DR。NBMA 网络通过指定邻居单播报文，点到多点网络多播报文。

模式：接口配置模式

命令：ip ospf network <type>

配置接口链路的网络类型

命令：no ip ospf network

恢复接口链路的网络类型为缺省值

参数：type 可选择 broadcast、non-broadcast、point-to-point、point-to-multipoint [non-broadcast]；第一种类型是广播网络，第二种类型为非广播网络，也即 NBMA，第三种类型是点到点网络，第四种类型是点到多点网络；点到多点网络又分为广播型和非广播型网络，非广播型邻居不能自动发现，必须指定邻居。

缺省：为广播网络

14.2.11 配置 hello 报文发送时间间隔

Hello 报文用于周期性发至邻居路由器，发现与维持邻居关系，选举 DR 及 BDR。Hello 报文的间隔可以手工配置，但需注意保持网络中邻居间的 hello 计时器间隔一致。Hello 计

时器的值与路由器收敛速度、网络负荷成反比。

模式：接口配置模式

命令：ip ospf hello-interval <seconds>

配置 hello 计时器的间隔

命令：no ip ospf hello-interval

恢复 hello 计时器间隔为缺省值

参数：seconds取值 1~(2^{16}-1)之间，表示两次hello报文发送之间的时间间隔。

缺省：在广播网络和点到点网络上 hello 间隔 10 秒；在 NBMA 网络和点到多点网络上 hello 间隔 30 秒。

14.2.12 配置邻居路由器失效时间

模式：接口配置模式

命令：ip ospf dead-interval <seconds>

配置邻居失效时间

命令：no ip ospf dead-interval

恢复邻居失效时间为缺省值

参数：seconds取值 1~(2^{16}-1)之间，表示经过seconds时间未接收到邻居的hello报文则认为该邻居已失效；每次接收到hello报文时均会更新邻居的dead计时器。

缺省：广播网络和点到点网络上邻居失效时间为 40 秒；在 NBMA 网络和点到多点网络上邻居失效时间为 120 秒；当修改了网络类型后，hello 间隔和 dead 间隔将使用缺省值。

14.2.13 配置重传时间

OSPF 是可靠的链路状态协议，表现在其交互的 LSU 报文均需要对端的应答 LSU-ack。当接收到确认报文时，方认为链路状态更新被接收。若在重传间隔内没有收到确认报文就会

向邻居重传这条 LSA。重传间隔可手工配置，需大于一个报文在两台路由器之间传送一个来回的时间，若设置的太小，会引起不必要的重传。

模式：接口配置模式
命令：ip ospf retransmit-interval <seconds>
配置接口的重传间隔
命令：no ip ospf retransmit-interval
恢复重传间隔为缺省值

参数：seconds取值 1~(2^{16}-1)之间，表示当对端未接收到LSA时需要重传的间隔。
缺省：重传间隔 5s

14.2.14 配置接口延时

在链路状态更新报文 LSU 中每条链路状态广播 LSA 均有 age 时间域，在传送前需要增加发送接口的传输时延。该参数主要考虑接口发送报文需要的时间，尤其在低速网络上需要考虑配置该参数。

模式：接口配置模式
命令：ip ospf transmit-delay <seconds>
设置接口的传输延时

命令：no ip ospf transmit-delay
恢复接口的传输延时为缺省值

参数：seconds取值 1~(2^{16}-1)之间，表示在该接口发送的LSA的age域需要增加这个时延值。
缺省：接口的传输时延 1s

14.2.15 配置接口在 DR 选举中的优先级

在广播网络中为避免重复的点到点之间传送链路信息，需要选举出指定路由器 DR 及 BDR 负责广播网段内的链路信息。接口的优先级表示其在选举 DR 时所具有的资格，当选举发生冲突时，优先级高的首先考虑。优先级为 0 不参与选举，优先级大于 0 均是候选人，每台路由器在各自的 hello 报文中包含自己的优先级信息及自己认为的 DR，在广播网络中广播，最后选择优先级大的成为 DR。若优先级相等则比较 router ID 大者优先。

当 DR 失效后，网络中路由器又需要经历一个重新选举 DR 的过程，这需要一个时间，且在这段时间内会引起路由计算错误。BDR 的概念就是为了平滑得过渡到新的 DR。BDR 是 DR 的备份，在 DR 选举中同时选出，它也和网络中其他路由器建立邻接关系，只是网络中信息的收集与发布结点在 DR 而非 BDR，BDR 仅维护邻接的同步。当 DR 失效后，BDR 会立即成为 DR，负责收集网段内信息，而此时会启动新的过程选举 BDR，但 BDR 的选举不影响路由的计算。

模式：接口配置模式

命令：ip ospf priority <prio>

配置接口在 DR 选举中的优先级

命令：no ip ospf priority

恢复接口优先级为缺省值

参数：prio 取值 0~255，表示 DR 选择中的优先级，当为 0 时表示不参与选举。

缺省：优先级为 1

14.2.16 配置接口上发送报文的代价

网络中通过配置不同链路不同的代价来控制流量，接口的代价表示从该接口发送报文的花费。若不手工配置则 OSPF 会根据接口波特率自动计算接口代价。

模式：接口配置模式

命令：ip ospf cost <cost>

命令：no ip ospf cost

参数：cost取值 1~(2^{16}-1)之间，表示该接口上发送报文的代价值。

缺省：接口代价 10

14.2.17 配置接口发送 DD 报文是否填 MTU 域

模式：接口配置模式

命令：ip ospf mtu-ignore

设置不检查 DD 报文中 mtu 值

命令：no ip ospf mtu-ignore

取消不检查 DD 报文中 mtu 值

缺省：检查 DD 报文中 mtu 值

14.2.18 配置接口报文认证

OSPF协议在接口上的报文认证支持明文方式和MD5方式。

模式：接口配置模式

命令：ip ospf authentication <mode>

配置认证模式

命令：no ip ospf authentication

取消认证

参数：无参数表示明文认证；message-digest表示MD5认证；null表示无认证

命令：ip ospf authentication-key <password>

配置明文认证密码串

命令：no ip ospf authentication-key

取消明文认证密码串

参数：password 表示明文认证的密码字符串

命令：ip ospf message-digest-key <key-id> md5 <password>

配置 MD5 认证密码

命令：no ip ospf message-digest-key <key-id>

取消 MD5 认证密码

参数：key-id 取值 1~255 之间，用于在密钥链中排序；password 表示密码字符串。

缺省：未配置任何认证

14.2.19 配置区域虚链路

OSPF 协议采用分层思想，将自治系统内的路由器划分成不同的组，这些组称之为区域，所有的区域并非平等并列，而是具有层次关系，其中 0.0.0.0 区域最特殊，为骨干区域，其他非骨干区域必须通过骨干区域来交换域间路由。所以所有非骨干区域必须与骨干区域连通，也即 ABR 上至少有一个接口在区域 0 中。如果因为网络拓扑的限制，某些区域无法与骨干区域保证物理上的通路，那么需要配置虚链路来保证逻辑上的通路。虚链路的两端都是 ABR，中间通过一个非骨干区域，被称为传输区域 transit area。配置虚链路时需指定传输区域的 ID 及对端 ABR 的 ID，且必须在两端的 ABR 上均配置方能生效。

当传输区域的路由被计算出来后虚链路被激活，则其在逻辑上相当于两个端点之间形成了一个点到点的连接，因此可以在其物理接口上配置接口的参数及启动认证功能。

ABR 之间传送的是单播报文，传输区域内转发该单播报文的路由器将其视作普通的 IP 报文来转发，因此可仅仅理解为传输区域内提供了一条逻辑链路，两台 ABR 之间可以交换协议报文。

模式：OSPF 配置模式

命令：area <area-id> virtual-link <router-id>

配置虚链路的传输区域及对端ID

[authentication <mode> |

配置虚链路的认证模式

authentication-key <password> |

配置虚链路明文认证密码

message-digest-key <key-id> md5 <password> |

配置虚链路MD5认证密码

hello-interval <seconds> |

配置虚链路的hello间隔

dead-interval <seconds> |

配置虚链路邻居失效时间

retransmit-interval <seconds> |

配置虚链路重传间隔

transmit-delay <seconds> |

配置虚链路接口时延

命令：no area <area-id> virtual-link <router-id>

[authentication <mode> |

authentication-key <password> |

message-digest-key <key-id> md5 <password> |

hello-interval <seconds> |

dead-interval <seconds> |

retransmit-interval <seconds> |

transmit-delay <seconds>]

取消虚链路设置

参数：area-id表示传输区域的ID，可以使用点分十进制格式A.B.C.D，也可以使用整型数格式，取值 0~(2^{32}-1)之间。router-id表示虚链路对端路由器的ID，使用A.B.C.D格式。认证及发送接口属性均为可选项，可参考相关命令说明。

缺省：不配置虚链路

14.2.20 配置区域路由聚合

模式：OSPF 配置模式

命令：area <area-id> range <ip-prefix> [advertise | not-advertise]

配置聚合范围

命令：no area <area-id> range <ip-prefix> [advertise | not-advertise]

取消聚合

参数：area-id表示区域ID，指定聚合该区域内路由，可以使用点分十进制格式A.B.C.D，也可以使用整型数格式，取值 0~(2^{32}-1)之间。Ip-prefix使用前缀格式A.B.C.D/M表示聚合范围。可选参数advertise和not-advertise表示是否广播聚合范围，也即ip-prefix。原有的网络路由均会广播。

14.2.21 配置区域报文认证

一个区域中所有路由器的认证类型需保持一致。一个网段中所有路由器的认证密码串需保持一致。配置区域认证仅启动认证功能（明文或者 MD5），密码使用接口的相应配置值。可参考接口报文认证配置。

模式：OSPF 配置模式

命令：area <area-id> authentication [message-digest]

配置区域认证模式

命令：no area <area-id> authentication

取消区域认证

参数：area-id表示区域ID，指定需认证的区域；可以使用点分十进制格式A.B.C.D，也可以使用整型数格式，取值 0~(2^{32}-1)之间。可选参数无表示明文认证，带message-digest表示MD5 认证。

缺省：不启动区域认证

14.2.22 配置 stub 区域

模式：OSPF 配置模式

命令：area <area-id> stub [no-summary]

配置路由器在 stub 区域内

命令：no area <area-id> stub [no-summary]

取消路由器在 stub 区域的属性

命令：area <area-id> default-cost <cost>

配置连接在 stub 区域的 ABR 广播路由的缺省代价

命令：no area <area-id> default-cost

恢复缺省代价为默认值

参数：area-id表示区域ID，指明哪个区域属性为stub；可以使用点分十进制格式A.B.C.D，也可以使用整型数格式，取值 0~(2^{32}-1)之间。no-summary表示不将域间路由注入stub区域。

第一组命令是配置位于 stub 区域内的路由器，第二组命令是配置有连接到 stub 区域的

接口的 ABR。

缺省：不配置 stub 区域

14.2.23 配置 nssa 区域

模式：OSPF 配置模式

命令：area <area-id> nssa [options]

配置 nssa 属性

命令：no area <area-id> nssa [options]

取消 nssa 区域属性

参数：area-id 表示区域 ID，options 详见命令手册。

缺省：不配置 nssa 区域

14.2.24 配置外部路由聚合

从其他协议引入的路由是一条一条放在 type-5 的 LSU 中广播的，使用聚合命令指定一个前缀范围，在这个范围内覆盖的路由均被抑止，只广播聚合后的这条路由。当外部路由数量巨大时，能有效的减少 LSDB 的规模。

模式：OSPF 配置模式

命令：summary-address <ip-prefix> [not-advertise | tag <tag>]

配置聚合范围及属性

命令：no summary-address <ip-prefix> [not-advertise | tag <tag>]

取消外部路由的聚合

参数：ip-prefix使用地址前缀格式A.B.C.D/M表示需要聚合的路由范围；not-advertise表示聚合后的路由不被广播；tag为设置的tag值，取值 0~(2^{32}-1)之间，缺省为 0。

缺省：不聚合外部引入的路由

14.2.25 配置外部路由的缺省权值

引入外部路由时，若 redistribute 命令不指定 metric 值，使用缺省权值。

模式：OSPF 配置模式

命令：default-metric <metric>

配置引入外部路由时的缺省权值

命令：no default-metric [metric]

恢复引入外部路由时缺省权值为默认值

参数：metric取值 0~(2^{24}-1)之间

缺省：缺省权值为 1

14.2.26 显示信息

模式：普通模式或特权模式

命令：show ip protocols

命令：show ip protocols ospf

显示OSPF协议信息

命令：show ip ospf [process-id]

显示OSPF进程信息

参数：instance-id为进程号，

取值0-(2^{16}-1)之间。

命令：show ip ospf border-routers

显示ABR信息

命令：show ip ospf database <type>

显示LSDB信息

参数：type为各类型LSA及汇总信息，详见命令手册。

命令：show ip ospf interface [if-name]

显示OSPF接口信息

参数：if-name为约定的三层接口名

命令：show ip ospf route [count]

显示OSPF路由表

参数：count表示显示路由表总条目数

命令：show ip ospf virtual-links

显示OSPF虚连接信息

命令：show ip ospf neighbor [options]

显示OSPF邻居信息

参数：options详见命令手册

模式：特权模式

命令：show running-config

显示交换机当前配置，包括OSPF配置。

命令：show running-config ospf

显示OSPF协议的当前配置。

14.3 OSPF 配置示例

(1) 配置

三台交换机两两相连，分别有6 个网段，都启用OSPF 协议，实现三台PC 机之间能够两两互通。要求接口在同一区域area 0。

在交换机1上：

```
Switch#configure terminal
Switch(config)#router ospf 100
Switch(config-ospf-100)#network 10.1.1.0/24 area 0
Switch(config-ospf-100)#network 10.1.2.0/24 area 0
Switch(config-ospf-100)#network 192.168.1.0/24 area 0
```

在交换机2上：

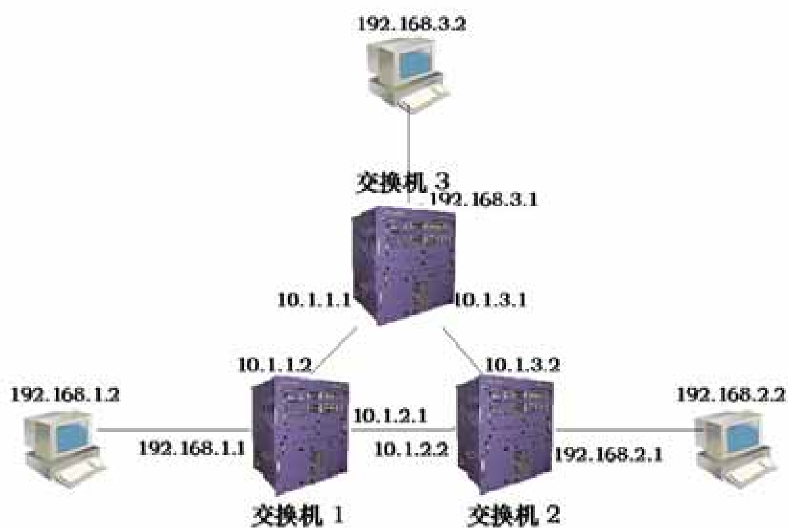
```
Switch#configure terminal
Switch(config)#router ospf 100
Switch(config-ospf-100)#network 10.1.2.0/24 area 0
Switch(config-ospf-100)#network 10.1.3.0/24 area 0
Switch(config-ospf-100)#network 192.168.2.0/24 area 0
```

在交换机3上：

```
Switch#configure terminal
Switch(config)#router ospf 100
Switch(config-ospf-100)#network 10.1.1.0/24 area 0
```

Switch(config-ospf-100)#network 10.1.3.0/24 area 0

Switch(config-ospf-100)#network 192.168.3.0/24 area 0



(2) 验证

show ip ospf database

show ip ospf interface

show ip ospf neighbor

show ip route ospf

show ip ospf route

第15章 配置VRRP

本章主要包括以下内容：

- VRRP 介绍
- VRRP 配置
- VRRP 配置示例

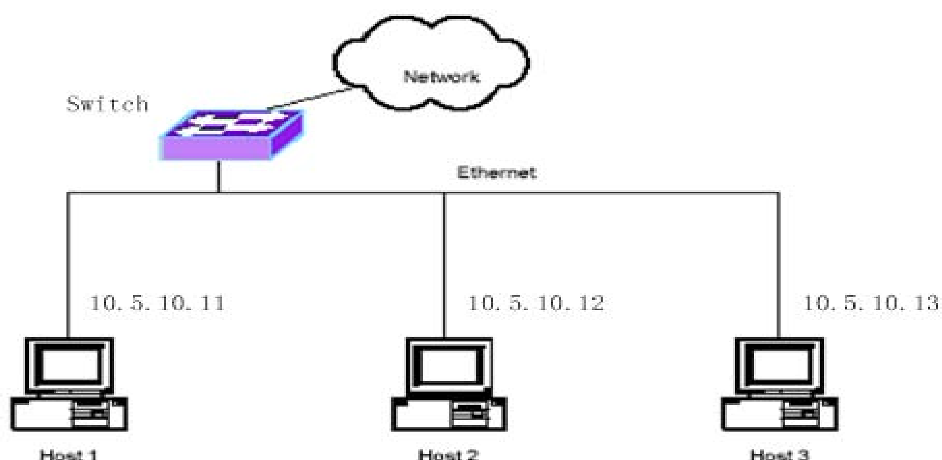
15.1 VRRP 介绍

VRRP 是虚拟路由器冗余协议的简称，是一个重要的三层可靠性协议，用于缺省网关的冗余备份。本节对 VRRP 协议进行一个详细的描述，主要包括以下内容：

- VRRP 概述
- VRRP 术语
- VRRP 协议交互
- 虚拟主路由器的选举
- 虚拟路由器的状态
- VRRP 跟踪

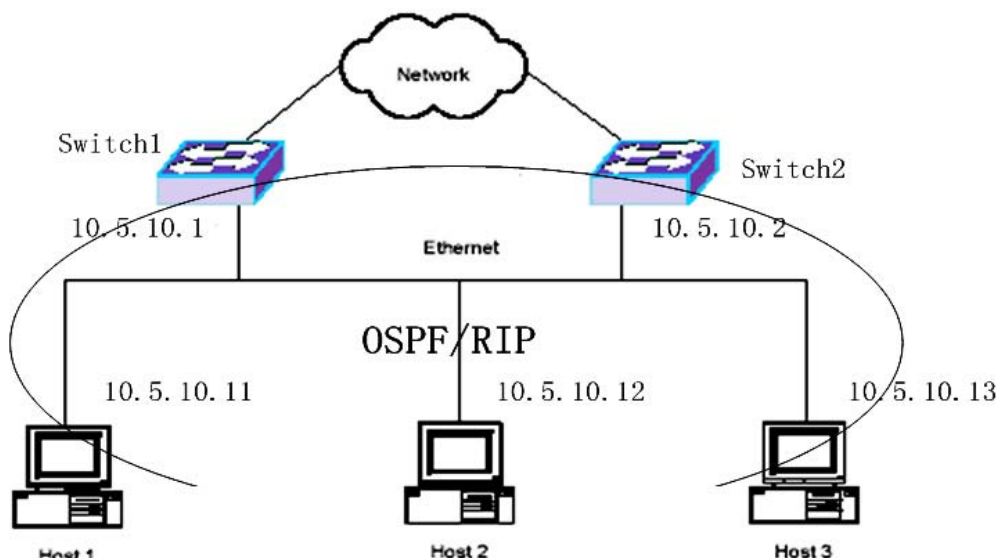
15.1.1 VRRP 概述

下图是一个典型的内部网组网方案。交换机的一个接口与外部网络相连，一个接口与内部网络相连，与内部网相连的接口的 IP 地址是 10.5.10.1，主机 1，2，3 都配置了 IP 地址，都在网段 10.5.10.0/24 内。主机 1，2，3 上都配置了一个默认网关，下一跳指向交换机，下一跳的 IP 地址是 10.5.10.1。这样，主机发送一个目的 IP 地址不在本网段内的报文会匹配缺省路由而发送到交换机，交换机再把报文转发出去，交换机也把外部网络发来的报文转发给相应的主机，这样主机就实现了与外部网络的通信。



在上面这种组网方案中，主机与外部网络之间的通信只能通过这个唯一的交换机，当交换机出现故障时，所有的主机都与外部中断。为了解决这个问题，有一种解决方案就是

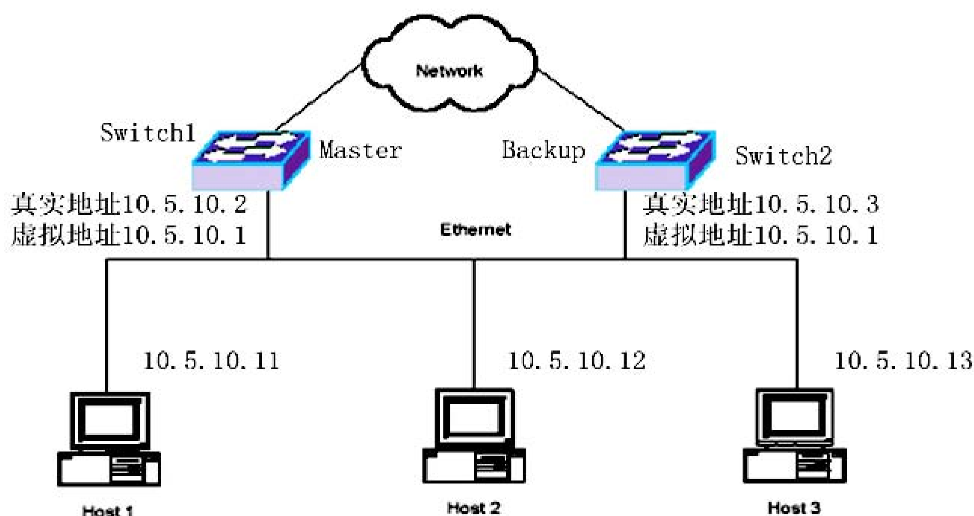
把一台交换机扩展为两台或多台交换机，在主机和交换机之间都运行动态路由协议 OSPF 或 RIP，如下图。



当主机运行了动态路由协议后，主机上能够学习到外部网络所有的路由，主机在与外部网络的通信时，根据报文的目的 IP 地址查找路由得到下一跳来决定报文是发送给 switch1 还是 switch2。当其中的一台交换机出现故障时，主机中的路由在很短的时间内能够重新学习，路由的下一跳会指向没有故障的路由器，这样，主机与外部网络的通信不会中断。

但是，在主机上实现动态路由协议是不现实的。对于主机来说，运行动态路由协议负载太大，对于网络来说，主机上运行动态路由协议会造成网络上过多的不必要的数据流量，况且有些主机根本就不支持动态路由协议。

为了根本解决这个单点故障的问题，VRRP 协议是最好的选择。VRRP 协议是专门针对这个问题而提出来的。如下图所示，Switch1 和 Switch2 组成一个虚拟路由器，两个交换机的接口的真实 IP 地址是不一样的，但是有一个共同的虚拟 IP 地址 10.5.10.1，主机的默认网关设置为虚拟 IP 地址 10.5.10.1。当 Switch1 是虚拟主交换机时，主机与外部网络的通信是通过 Switch1 来转发，但当 Switch1 出现故障时，Switch2 接替 Switch1 成为虚拟主交换机，主机与外部网络的通信通过 Switch2 来转发。使用 VRRP 协议，主机只需要设置默认网关，而不需要在主机上运行别的协议，主机的负载小，而网络上只需要增加很少的 VRRP 协议流。



15.1.2 VRRP 术语

下面介绍几个经常要用到的术语：

1）VRRP

Virtual Router Redundancy Protocol 的缩写，虚拟路由器冗余协议，是一种缺省网关的容错协议，可提高网络的可靠性。

2）Virtual Router

虚拟路由器，一个抽象对象，基于子网接口，包括一个虚拟路由器标识符（VRID）和一个或多个 IP 地址，这个（些）IP 地址又称为虚拟 IP 地址，虚拟 IP 地址作为主机的默认网关。

3）VRRP Router

VRRP 路由器，即运行 VRRP 协议的路由器，一个 VRRP 路由器可以加入到一个或多个虚拟路由器中。

4）IP Address Owner

IP 地址拥有者，虚拟路由器的虚拟 IP 地址与接口的真实 IP 地址相同的 VRRP 路由器。

5）Virtual Router Master

虚拟主路由器,负责转发通过虚拟路由器的三层数据包,对虚拟路由器的 IP 地址的 ARP 请求进行回应。如果某个 VRRP 路由器是 IP 地址拥有者，则它总是虚拟主路由器。

6）Virtual Router Backup

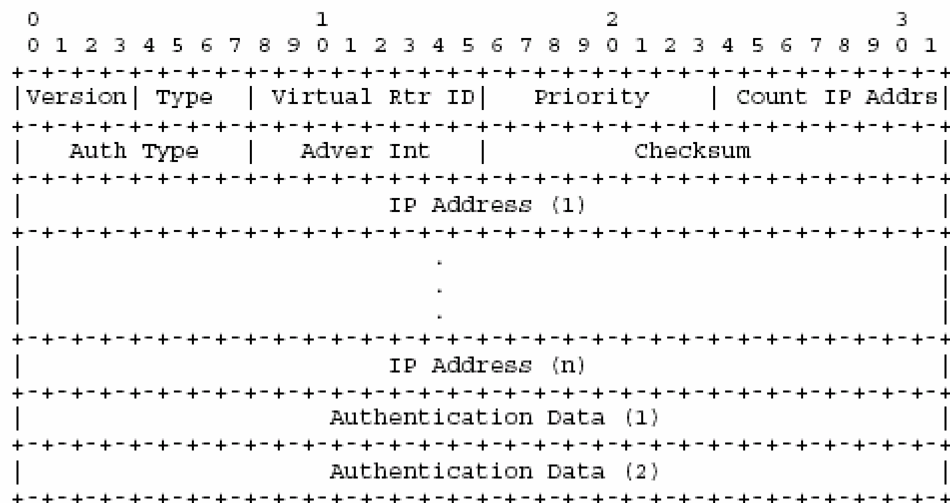
虚拟备份路由器，不转发三层数据包，不应答虚拟 IP 地址的 ARP 请求，当虚拟主路由器出现故障时接替虚拟主路由器的工作。

为了更好地理解这几个术语，要注意以下几点：

- 一个交换机可包括多个接口，可在多个接口子网上启动 VRRP 协议。
- 一个接口子网上可存在一个或多个虚拟路由器。
- 一个 VRID 标识一个虚拟路由器，在一个接口子网上不同的虚拟路由器的 VRID 不同。
- 在一个交换机上的不同接口子网上的虚拟路由器的 VRID 可以相同。

15.1.3 VRRP 协议交互

VRRP 协议包封装在 IP 包内，VRRP 报文头如下图：



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Type  | Virtual Rtr ID|   Priority    | Count IP Addrs|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Auth Type   |   Adver Int   |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         IP Address (1)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            .                                  |
|                            .                                  |
|                            .                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         IP Address (n)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Authentication Data (1)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Authentication Data (2)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

1）VRRP 包的 MAC 帧头字段

源 MAC 地址： 虚拟路由器的虚拟 MAC 地址，为 00-00-5e-00-01-{VRID}，VRID 是虚拟路由器标识符。例如虚拟路由器的 VRID 为 1，则虚拟 MAC 地址为 00-00-5e-00-01-01。

目的 MAC 地址：VRRP 组播 MAC 地址，为 01-00-5e-00-00-12。

2）VRRP 包的 IP 包头字段

源 IP 地址：发送 VRRP 包的接口的主 IP 地址。

目的 IP 地址：组播 IP 地址 224.0.0.18，不能够做三层转发。

TTL：255，为了防止远端 VRRP 包攻击。

Protocol：112。

3）VRRP 包头字段

Version：2。

Type：VRRP 包的类型，只支持一种类型：1 --- ADVERTISEMENT，VRRP 通告包。

VRID：标识一个虚拟路由器。

Priority：对于此虚拟路由器来说，发送的 VRRP 路由器的优先级。

Count IP Addrs：虚拟 IP 地址的个数，一个虚拟路由器中可以有多个虚拟 IP 地址。

Auth Type：一个虚拟路由器中的 VRRP 路由器之间的认证方法。

Advertisement Interval：通告的间隔时间，缺省为 1 秒。

Checksum：校验和，从 VRRP 包头的 Version 算起。

IP Address(es)：一个或多个虚拟 IP 地址。

Authentication Data：认证的数据。

4）VRRP 优先级

一个虚拟路由器中的每一个 VRRP 路由器都需要配置一个优先级 priority。优先级的范围从 0 到 255，其中 0 和 255 有特殊的用途，可配置的优先级范围从 1 到 254，缺省为 100。优先级的值越大，优先级越高，越有可能成为虚拟主路由器。

在一个虚拟路由器中当某个 VRRP 路由器是 IP 地址拥有者时，它的优先级是 255。

当虚拟主路由器需要通告给其它备份路由器它不再是主时，发送优先级为 0 的 VRRP 包给其它备份路由器，这样可以快速触发其它备份路由器成为虚拟主路由器。

5）VRRP 认证

VRRP 协议提供了三种认证方法，在实际使用时可以根据网络的安全性要求来选择不同

的认证方法。

0 --- No Authentication

不做认证

1 --- Simple Text Password

简单口令认证

2 --- IP Authentication Header

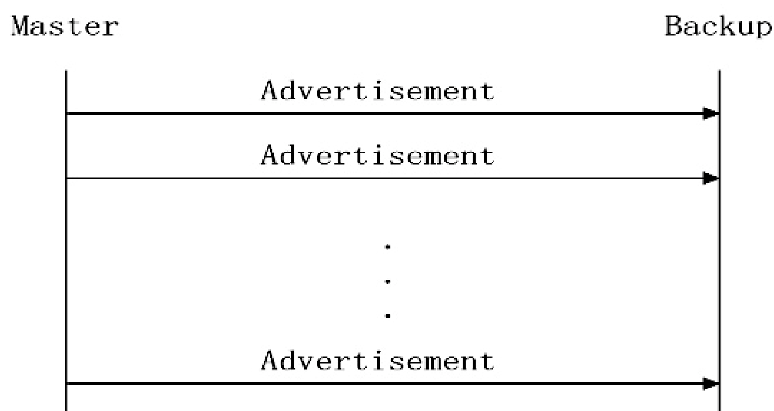
IP 认证头，通过 HMAC-MD5 方法计算消息摘要

在安全性不高的网络可以采用不做认证或简单口令认证方法，在安全性高的网络采用 HMAC 认证方法。

对于 0 和 2 认证方法，Authentication Data 字段填 0，对于 1 认证方法， Authentication Data 字段填口令。对于 2 认证方法，消息摘要填在 IP Authentication Header 字段，也就是说在 IP 头加上 AH 字段。

6）VRRP 包交互

VRRP 协议只有一种类型的包，ADVERTISEMENT 通告包。在一个虚拟路由器中，虚拟主路由器每隔 Advertisement Interval 时间（缺省为 1 秒）发送一个通告包。虚拟备份路由器根据收到的 VRRP 通告包来决定是否需要状态迁移。主与备的协议交互如下图：



15.1.4 虚拟主路由器的选举

在一个虚拟路由器中虚拟主路由器的选择由以下因素来决定：

- IP 地址所有者

如果一个 VRRP 路由器是 IP 地址所有者（它的接口 IP 地址与虚拟 IP 地址相同），如果该路由器工作正常，它就是虚拟主路由器。

- VRRP 优先级

工作正常的优先级最高的 VRRP 路由器成为虚拟主路由器。可配的优先级范围从 1 到 254，IP 地址所有者的路由器的优先级为 255，当虚拟主路由器通知虚拟备份路由器自己不再是主时，在 VRRP 包中给定优先级 0。

- 接口的实际 IP 地址大小，当优先级相同时，接口的实际 IP 地址大的 VRRP 路由器成为虚拟主路由器。

在以下情况下，虚拟路由器中会出现主备切换：

1）当虚拟主路由器出现故障时，会出现主备切换，这种情况下又有两种可能性：

- 如果虚拟主路由器还能够活动，会发送一个优先级为 0 的 VRRP 包，备份路由器收到这个包后在 Skew_Time 时间内没有收到虚拟主路由器的 VRRP 包后会切换为虚拟主路由器。这种情况切换速度比较快，在 1 秒以内能够实现切换。
- 如果虚拟主路由器不能活动，虚拟备份路由器在 Master Down Interval 时间内没有收到虚拟主路由器的 VRRP 包后会切换为虚拟主路由器。

Master_Down_Interval = (3 * Advertisement_Interval) + Skew_Time

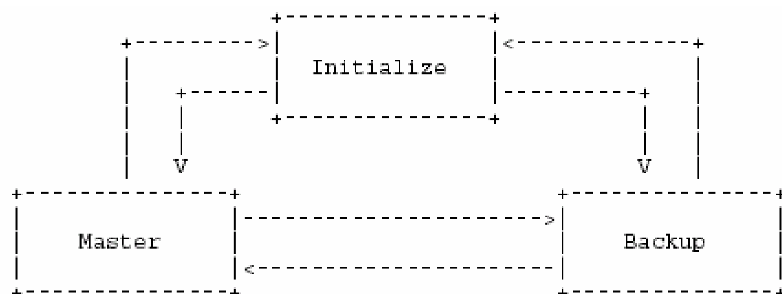
Skew_Time = ((256 – Priority) / 256)

2）当虚拟主路由器不是 IP 地址拥有者，而现在有一个 IP 地址拥有者的路由器加入网络，此时该路由器会成为虚拟主路由器，出现主备切换。

3）当一个 VRRP 路由器加入网络，如果该路由器的优先级比虚拟主路由器还高并且是抢占模式（配置变量 Preempt_Mode 为 TRUE）时，该路由器会成为虚拟主路由器，出现主备切换。

15.1.5 虚拟路由器的状态

在一个虚拟路由器中的每一个 VRRP 路由器都执行一个状态机。状态机的迁移如下图：



1）Initialize 状态

Initialize 状态是一个虚拟路由器的初始状态，在这种状态下等待 Startup 启动事件。如果在这种状态下收到 Startup 事件时处理如下：

- 如果此 VRRP 路由器的优先级是 255（也就是 IP 地址拥有者），该路由器成为虚拟主路由器，迁移到 Master 状态。
- 否则，该路由器成为虚拟备份路由器，迁移到 Backup 状态。

路由器迁移到 Master 状态后做的动作如下：

- 发送一个 VRRP 通告包。
- 广播一个 ARP 请求，包含虚拟 IP 地址和对应的虚拟 MAC 地址。
- 设置 Adver_Timer 定时器，定时间隔为 Advertisement_Interval。

路由器迁移到 Backup 状态后做的动作如下：

- 设置 Master_Down_Timer 定时器，定时间隔为 Master_Down_Interval。

2）Backup 状态

Backup 状态的目的是监控虚拟主路由器的可用性和状态，随时接替虚拟主路由器的工作。

如果收到一个 Shutdown 事件，取消 Master_Down_Timer 定时器，回到 Initialize 状态。

如果 Master_Down_Timer 到期，成为虚拟主路由器，迁移到 Master 状态。

如果收到一个 VRRP 通告包，存在以下几种情况：

- 如果 VRRP 包中的优先级字段为 0，设置 Master_Down_Timer，定时间隔为 Skew_Time。
- 否则，如果抢占模式（Preempt_Mode）为 FALSE 或者 VRRP 包中的优先级 >= VRRP 路由器的优先级，重设 Master_Down_Timer，定时间隔为 Master_Down_Interval。
- 否则，丢弃 VRRP 包。

3）Master 状态

处于 Master 状态的 VRRP 路由器负责转发通过虚拟路由器的三层数据包。

如果收到 Shutdown 事件，取消 Adver_Timer 定时器，发送一个优先级为 0 的 VRRP 通告包，迁移到 Initialize 状态。

如果 Adver_Timer 定时器到期，发送一个 VRRP 通告包，重设 Adver_Timer 定时器。

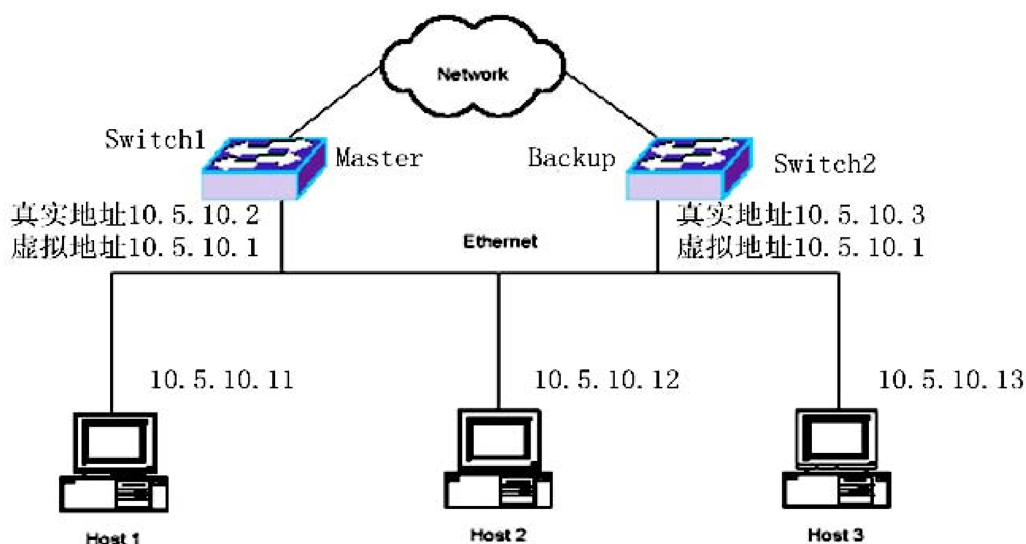
如果收到一个 VRRP 通告包，存在以下几种情况：

- 如果包中优先级为 0，发送一个 VRRP 通告包，重设 Adver_Timer。
- 否则如果包中的优先级大于 VRRP 路由器的优先级或优先级相同,但发送该包的 IP 地址大于 VRRP 路由器的接口主 IP 地址时，取消 Adver_Timer 定时器，设置 Master_Down_Timer，迁移到 Backup 状态。
- 否则，丢弃该 VRRP 通告包。

15.1.6 VRRP 跟踪

VRRP 协议本身只能检测虚拟路由器内部的故障，如虚拟路由器所在的接口 LINK DOWN 或 VRRP 路由器死机等，而检测不到虚拟路由器外部的故障。当虚拟路由器外部出现故障时，虚拟路由器不能根据这些故障进行虚拟主路由器的选择，这样会造成网络数据的中断。VRRP 跟踪可以解决此问题，VRRP 路由器对指定的外部事件进行跟踪，当出现外部故障时 VRRP 路由器改变自己的运行优先级，重新选择虚拟主路由器，保证网络数据不中断。

如下图，当虚拟主路由器 Switch1 的外部接口 LINK DOWN 时，如果没有启用 VRRP 跟踪功能，Switch1 不能检测到此外部故障，Swith1 继续是虚拟主路由器，主机不能访问外部网络。如果启用了 VRRP 跟踪功能，Switch1 能够发现外部故障，并且修改自己的运行优先级，重新进行虚拟主路由器的选择，Switch1 改变为虚拟备份路由器，Switch2 改变为虚拟主路由器，这样主机可以继续访问外部网络。



VRRP 跟踪包括接口跟踪，路由跟踪和 PING 跟踪三种类型。接口跟踪是 VRRP 路由器跟踪虚拟路由器外部的接口，如果跟踪的某个接口 LINK DOWN 时，表明出现了外部故障。路由跟踪是 VRRP 路由器跟踪其所学习到的路由表中的路由，如果路由不存在或者路由存在但不是激活状态，表明出现了外部故障。PING 跟踪是 VRRP 路由器一直 PING 被跟踪的设备，如果在规定的时间内，设备没有 PING 应答，则表明出现了外部故障。虚拟路由器可以同时对接口、路由和 PING 进行跟踪，对于每一类跟踪，又可以跟踪多个事件，只要被跟踪的一个事件出现了故障，则表明虚拟路由器出现了外部故障，只有所有的被跟踪的事件是正常的，才表明虚拟路由器没有外部故障。

15.2 VRRP 配置

VRRP 配置包括以下内容：

- 创建和删除虚拟路由器
- 配置虚拟路由器的虚拟 IP 地址
- 配置虚拟路由器的参数
- 配置 VRRP 跟踪
- 启动和关闭虚拟路由器
- 查看 VRRP 信息

15.2.1 创建和删除虚拟路由器

虚拟路由器是建立在子网接口上的，并且需要指定一个 VRID。在同一个接口下，不能有两个相同 VRID 的虚拟路由器存在，而不同的接口下可以存在两个相同的 VRID 的虚拟路由器。理论上一个接口下最多可以创建 255 个虚拟路由器，而目前交换机只实现了一个接口下最多创建 4 个虚拟路由器。系统缺省情况下没有创建虚拟路由器。

当一个虚拟路由器不再需要使用时，可以删除此虚拟路由器，如果虚拟路由器已经启动了，则会先关闭虚拟路由器，再把虚拟路由器删除。

创建和删除虚拟路由器的命令如下：

命令	描述	CLI模式

router vrrp <if-name> <vrid>	在一个接口下创建一个虚拟路由器，并且进入VRRP配置模式，如果该虚拟路由器已经存在，则直接进入VRRP配置模式。第一个参数是VLAN接口名，第二个参数是VRID，范围从1到255。	全局配置模式
no router vrrp <if-name> [vrid]	删除一个接口下的所有虚拟路由器或指定的一个虚拟路由器。第一个参数是VLAN接口名，第二个参数是VRID，如果不输入第二个参数，则删除此接口下的所有虚拟路由器，如果输入第二个参数，则删除此接口下指定的虚拟路由器。	全局配置模式

注意：

- 在创建虚拟路由器之前，必须先保证接口已经存在并且在接口上已经配置了 IP 地址。
- 在删除 VLAN 接口、删除 VLAN 接口上的 IP 地址或修改 VLAN 接口的 IP 地址时，该接口上的所有虚拟路由器都会被删除。

15.2.2 配置虚拟路由器的虚拟 IP 地址

虚拟路由器上必须配置虚拟 IP 地址，理论上一个虚拟路由器可以存在一个或多个虚拟 IP 地址，但交换机在实现时一个虚拟路由器只支持一个虚拟 IP 地址。在配置时，一个虚拟路由器中的多个 VRRP 路由器必须配置相同的虚拟 IP 地址。缺省情况下交换机没有配置虚拟 IP 地址。

配置虚拟路由器的虚拟 IP 地址的命令如下：

命令	描述	CLI模式
vrrp ip-address <virtual-ip>	设置虚拟路由器的虚拟IP地址。	VRRP配置模式

no vrrp ip-address	删除虚拟路由器的虚拟IP地址。	VRRP配置模式

注意：

- 当需要修改虚拟路由器的虚拟 IP 地址时，必须先删除虚拟 IP 地址，再设置虚拟 IP 地址。
- 配置虚拟路由器的虚拟 IP 地址必须在虚拟路由器已经关闭的情况下才能成功，当虚拟路由器启动时不能配置成功。
- 设置的虚拟 IP 地址必须与接口的主 IP 地址在同一个网段，否则配置不成功。
- 主机 PING 不通虚拟 IP 地址，当对交换机进行网管时，使用交换机的真实的 IP 地址，不要用虚拟 IP 地址。

15.2.3 配置虚拟路由器的参数

虚拟路由器的参数包括优先级，抢占模式，通告时间间隔，认证方法和认证数据，这些参数都有缺省值，如下表：

参数	缺省值
优先级	100
抢占模式	TRUE
通告时间间隔	1 秒
认证方法	不做认证
认证数据	无

在配置时，对于虚拟路由器的多个 VRRP 路由器，通告时间间隔，认证方法和认证数据必须配置一样，而优先级和抢占模式参数可以配置一样，也可以配置不一样。

对于优先级，分为配置优先级和运行优先级，大部分情况下，运行优先级使用的是配置优先级，但当 VRRP 路由器是 IP 地址拥有者时，运行优先级为 255，不使用配置优先级。

对于认证方法，交换机目前只实现了不做认证和简单口令认证两种方式，而对于 IP 认证头方式没有实现。

配置虚拟路由器的参数的命令如下表：

命令	描述	CLI模式
vrrp priority <value>	设置虚拟路由器的优先级，优先级的范围为3到254，优先级1和2预留，有其它用途。	VRRP配置模式
vrrp preempt {true | false}	设置虚拟路由器的抢占模式，TRUE表示进行抢占，FALSE表示不进行抢占。	VRRP配置模式
vrrp advertisement-interval <interval>	设置虚拟路由器的通告时间间隔，范围从1到255,单位为秒。	VRRP配置模式
vrrp authentication none	设置虚拟路由器的认证方法为不做认证。	VRRP配置模式
vrrp authentication simple-password <key>	设置虚拟路由器的认证方法为简单口令认证，并且要设置认证数据，即口令。口令不能超过8个字节。	VRRP配置模式

注意：

- 配置虚拟路由器的参数必须在虚拟路由器已经关闭的情况下才能成功，当虚拟路由器启动时不能配置成功。

15.2.4 配置 VRRP 跟踪

目前交换机只实现了 VRRP 接口跟踪功能。VRRP 路由器可以同时跟踪一个或多个接口，接口可以是三层 VLAN 接口，也可以是二层接口。交换机缺省没有配置被跟踪的接口。

如果 VRRP 路由器是 IP 地址拥有者时，管理员可以配置 VRRP 跟踪，但实际上 VRRP 跟踪不会生效，也就是说即使虚拟路由器出现了外部故障，也不会重新选择虚拟主路由器。如果要使用 VRRP 跟踪功能，就不要把虚拟路由器配置成 IP 地址拥有者。

当管理员配置了 VRRP 跟踪，指定了要跟踪的一个或多个接口并且启动了虚拟路由器时，VRRP 跟踪就开始生效。当 VRRP 路由器发现被跟踪的一个接口 LINK DOWN 时，认为出现了外部故障，把虚拟路由器的运行优先级设置为 1，通过 VRRP 协议包的交互，可重新选择虚拟主路由器。当被跟踪的接口都是 LINK UP 时，故障恢复，虚拟路由器的运行优

先级重新设置为配置优先级。

配置 VRRP 跟踪的命令如下表：

命令	描述	CLI模式
vrrp tracking interface <if-name>	设置虚拟路由器要跟踪的接口，接口可以是三层接口，也可以是二层接口。	VRRP配置模式
no vrrp tracking interface [if-name]	清除虚拟路由器的被跟踪的接口，如果不带参数，清除所有被跟踪的接口，如果带参数，清除一个被跟踪的接口。	VRRP配置模式

注意：

配置 VRRP 跟踪必须在虚拟路由器已经关闭的情况下才能成功，当虚拟路由器启动时不能配置成功。

15.2.5 启动和关闭虚拟路由器

当创建了虚拟路由器并且设置了虚拟 IP 地址和参数后，虚拟路由器并没有真正运行，还处于 Initialize 状态。启动虚拟路由器会启动协议的运行，给协议发送一个 Startup 事件，状态机迁移到 Master 状态或者 Backup 状态。关闭虚拟路由器会关闭协议的运行，给协议发送一个 Shutdown 事件，状态迁回到 Initialize 状态。

在启动虚拟路由器前必须保证已经配置了虚拟 IP 地址。在虚拟路由器启动的情况下，如果需要修改虚拟 IP 地址或者参数，必须先关闭虚拟路由器再进行配置，配置完成后再启动虚拟路由器。

启动和关闭虚拟路由器的命令如下：

命令	描述	CLI模式
enable vrrp	启动虚拟路由器。	VRRP配置模式
disable vrrp	关闭虚拟路由器。	VRRP配置模式

15.2.6 查看 VRRP 信息

通过命令可以查看到 VRRP 的运行状态信息和配置信息,查看 VRRP 信息的命令如下:

命令	描述	CLI模式
show vrrp [if-name] [vrid]	如果不输入参数,显示所有的虚拟路由器的信息,如果只输入第一个参数,显示某个接口下的虚拟路由器的信息,如果输入两个参数,则显示某个接口下的指定的虚拟路由器。	普通模式,特权模式
show running-config	查看系统的当前配置,可以查看到VRRP的配置。	特权模式

15.3 VRRP 配置示例

(1) 配置

在两台交换机上启用VRRP功能,为局域网中的用户提供三层路由冗余功能,消除网络中的路由故障,设置交换机1为主用交换机Master,交换机2为备份交换机Backup。



交换机1上的配置：

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp vlan2 1
Switch(config-vrrp)#vrrp ip-address 192.168.1.1
Switch(config-vrrp)#enable vrrp
```

交换机2上的配置：

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
```

```
Switch(config-ge1/1)#exit
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.2/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp vlan2 1
Switch(config-vrrp)#vrrp ip-address 192.168.1.1
Switch(config-vrrp)#enable vrrp
```

(2) 验证:

通过以下命令查看VRRP的信息：

```
show running-config
show vrrp
show vrrp vlan2
```

第16章 配置VLLP

本章主要包括以下内容：

- VLLP 介绍
- VLLP 配置
- VLLP 配置示例

16.1 VLLP 介绍

VLLP（VRRP 二层环路保护协议 VRRP Layer-2 Loop Protect Protocol）是为解决 VRRP 协议应用中出现的二层环路问题而提出的私有协议。当使用两台三层交换机实现虚拟路由冗余备份时，三层交换机和二层交换机之间会构成环路，VLLP 协议通过报文交互，互相通知对方各自链路上的端口状态,并计算出环路将特定端口状态置为 block 从而切断环路。置为 block 状态的端口若计时器超时会重新置为 forward 状态。VLLP 协议通过即时通知端口状态变化和计时器超时来监测并维护端口的环路状态，并保证及时切断环路。VLLP 协议采用查询-应答方式来收集端口状态信息。当两台运行 VLLP 协议的三层交换机启动时，会自动选举一台处于发送者状态，另一台处于接收者状态。发送者负责定时发送查询报文，接收者接收到查询报文回送应答报文。当接收者有端口状态变化时需要主动发送链路状态变化报文来通知发送者作相应变化。VLLP 协议需要与 VRRP 协议协同工作，在 vlan 上启动并维护 vlan 内相关端口状态。VLLP 协议只需要运行于 VRRP 交换机上，而二层交换机不需要运行任何环路保护协议。目前 iSpirit8806 v3.0 版本提供的 VLLP v1.0 模块仅支持两台三层交换机之间的 VRRP 应用。

VLLP 协议基本概念：

VLLP 设备：在一个 vlan 上运行的一个 VLLP 协议实体称之为 VLLP 设备。

VLLP 端口：在 VLLP 设备对应的 vlan 内参与 VLLP 协议交互的端口。

VLLP 设备状态：VLLP 设备有发送者和接收者两种状态。

发送者：处于发送者状态的 VLLP 设备主动周期性的发送 VLLP 查询报文。

接收者：处于接收者状态的 VLLP 设备应答查询报文；当链路状态变化时主动发送 VLLP 链路状态变化报文。

VLLP 端口状态：VLLP 端口有 disable、block、forward 三种 STP 状态。

主端口：VLLP 设备处于发送者状态时选举一个 VLLP 端口作为主端口；一个 VLLP 发送者只有一个主端口。

VLLP 端口映射关系：存在与对端交换机进行 VLLP 协议报文交互的 VLLP 端口。

VLLP 设备接收者选举原则：

1.优先级高的成为接收者；

2.优先级相同，MAC 地址大的成为接收者。

主端口选举原则：

1.端口必须是 link up 的

2.VLLP 端口必须存在映射关系

若没有满足条件的 VLLP 端口则主端口不存在；

若有多个满足条件的 VLLP 端口只能选择一个作为主端口。

VLLP 端口状态确定原则：

VLLP 设备是发送者，那么主端口的状态必为 forward；

VLLP 设备是发送者，链路状态是 link up 且不存在映射关系的 VLLP 端口状态为 forward

VLLP 设备是发送者，链路状态是 link up 且存在映射关系的 VLLP 端口状态为 block；

VLLP 设备是接收者，链路状态是 link up 的 VLLP 端口状态为 forward；

链路状态为 link down 的 VLLP 端口状态为 disable。

VLLP 协议报文封装在 MAC 帧内

<table>
<tr><td colspan="6">Destination MAC Address (6 bytes)</td></tr>
<tr><td colspan="6">Source MAC Address (6 bytes)</td></tr>
<tr><td colspan="2">0x8100</td><td>Prio</td><td colspan="2">Vlan ID (12 bits)</td><td>Ethernet Type (2 bytes)</td></tr>
<tr><td>Version</td><td>Type</td><td colspan="3">Port1(2 bytes)</td><td></td></tr>
<tr><td>Priority</td><td>Query Inter</td><td colspan="3">Main port</td><td></td></tr>
<tr><td colspan="5">Reserved (4 bytes)</td><td></td></tr>
<tr><td colspan="2">Port2</td><td colspan="2">Link state</td><td>STP state</td><td></td></tr>
</table>

VLLP 协议报文有三种类型

链路状态查询报文 LQ

链路状态应答报文 LA

链路状态改变报文 LC

报文格式中各个域的取值范围：

Des MAC：固定为 00:09:ca:ff:ff:ff

Src MAC：发送 VLLP 协议报文的 vlan 的 MAC

Ethernet Type：固定为 0x268e

Version：当前为 1

Type：LQ 为 1；LA 为 2；LC 为 3；

Port1：发送 VLLP 协议报文的端口的索引值

Priority：VLLP 设备优先级，取值 1~255；

Query Interval：VLLP 发送者查询计时器间隔，缺省 5 秒；

Main port：VLLP 发送者主端口索引值，仅在 LQ 报文中；

Reserved：保留域为零

Port2：LC 报文中发生状态改变的端口的索引值，LQ 与 LA 报文中 port2 与 port1 一致；

Link state：port2 的链路状态，link up 为 1，link down 为 2；

STP state：port2 的 STP 状态，disable 为 1，block 为 2，forward 为 3。

VLLP 协议原理：

在一个 vlan 内配置 VLLP 设备并启动 VLLP 协议，在对端交换机相应的 vlan 内也配置 VLLP 设备并启动 VLLP 协议。这时在 vlan 上运行的 VLLP 协议实体（VLLP 设备）构成一对发送者与接收者。在协议启动时，双方均为发送者，都向对方发出 LQ 报文，当 VLLP 设备接收到 LQ 报文时会根据报文中携带的优先级及对端 MAC 地址进行接收者的选举，胜出的一方成为接收者，并且不再发送 LQ 报文而是应答发送者的 LQ 报文。当接收者的计时器超时还未接收到 LQ 报文时，接收者会重新回到发送者状态并开始发送 LQ 报文。

在启动了 VLLP 协议的 vlan 内，需要参与 VLLP 协议报文交互的端口需要配置为 VLLP 端口，VLLP 端口可以是有效的二层端口（包括 trunk 组），但 trunk 的成员不允许被配置为 VLLP 端口。VLLP 协议报文都是通过 VLLP 端口发送接收的。VLLP 端口和对端交换机相应的启动了 VLLP 协议的 vlan 内配置的 VLLP 端口构成一对映射关系，它们通过发送查询报文接收应答报文或者改变报文来确定与对端端口的这种映射关系，并根据这种映射关系和本身的链路状态来计算网络中可能存在的环路，依据 VLLP 端口的状态确定原则来维护端口的 STP 状态，从而阻止拓扑中的环路。

在启动了 VLLP 协议的 vlan 内可以启动多个 VLLP 端口，它们可能与对端交换机存在物理链接，也可能不存在。当端口属于多个 vlan 时，同一个 VLLP 端口也会出现在多个 VLLP 设备中。VLLP 协议会动态的收集 VLLP 端口链路状态变化的信息以及对端 VLLP 端口的 STP 状态来及时的计算环路并有效的阻止网络中环路的发生。

16.2 VLLP 配置

启动 VLLP 协议后可进行相关属性配置及端口创建，其相关命令均在 VLLP 配置模式下。

VLLP 的配置包括：

- 在三层接口上创建 vllp 设备
- 使能 vllp 设备
- 在二层接口上创建 vllp 端口
- 配置 vllp 设备优先级
- 配置 vllp 设备查询计时器间隔

16.2.1 在三层接口上创建 vllp 设备

模式：全局配置模式

命令：router vllp <if-name>　　创建 vllp 设备并进入 VLLP 配置模式

命令：no router vllp <if-name>　　删除 vllp 设备

参数：if-name 为约定的三层接口名（例如：vlan1 vlan2…）

缺省：不启动 vllp 协议

16.2.2 使能 vllp 设备

模式：VLLP 配置模式

命令：vllp enable　　使能 vllp 设备

命令：vllp disable　　禁止 vllp 设备

缺省：vllp 设备创建后并没有启动

16.2.3 在二层接口上创建 vllp 端口

模式：VLLP 配置模式

命令：vllp port <if-name>　　创建 vllp 端口

命令：no vllp port <if-name>　　删除 vllp 端口

参数：if-name 为约定的二层接口名（例如：ge1 ge2 trunk1…）

缺省：二层端口上并未应用 vllp 协议。当二层接口是 trunk 成员时不能应用 vllp 协议。

16.2.4 配置 vllp 设备优先级

模式：VLLP 配置模式

命令：vllp priority <priority>　　配置 vllp 设备优先级

命令：no vllp priority [priority]　　恢复 vllp 设备优先级为缺省值

参数：priority 取值在 1~255 之间。优先级用于 vllp 设备选举出接收者。

缺省：100

16.2.5 配置 vllp 设备查询计时器间隔

模式：VLLP 配置模式

命令：vllp query-interval <interval> 配置本地的查询计时器间隔

命令：no vllp query-interval [interval] 恢复查询计时器间隔为缺省值

参数：interval 取值为 1~255 之间。当 vllp 设备是发送者时或者迁移回发送者时配置值会生效。

缺省：5 秒

16.2.6 显示信息

模式：普通模式或特权模式

命令：show vllp

显示 vllp 协议的 vllp 设备列表

命令：show vllp <if-name>

显示某一 vllp 设备的详细信息

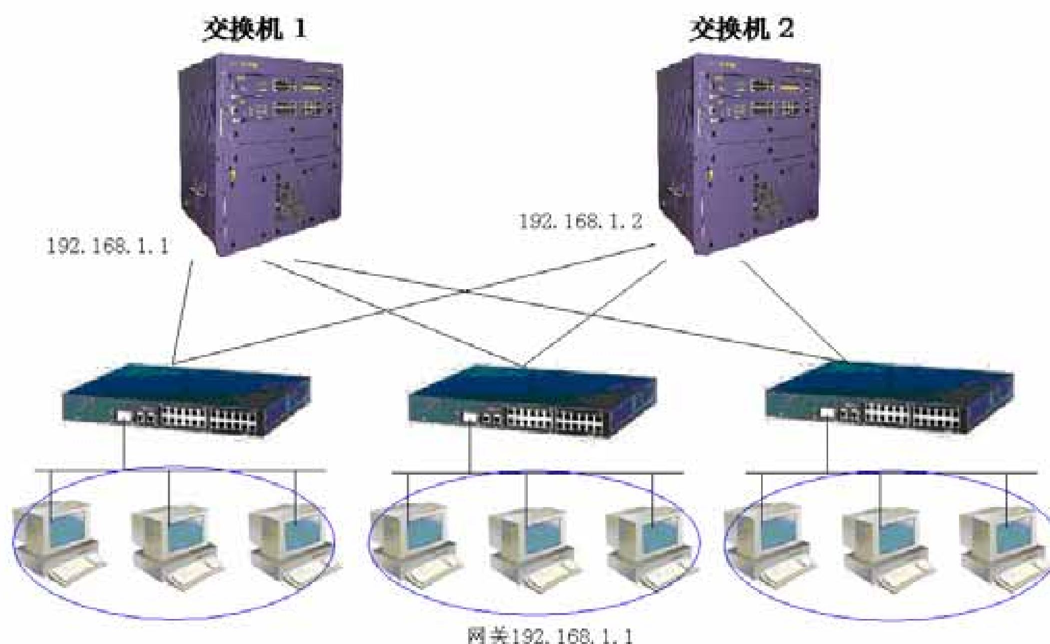
参数：if-name 为约定的三层接口名（例如：vlan1 vlan2…）

命令：show vllp map

显示 vllp 协议中各个 vllp 端口的映射关系

16.3 VLLP 配置示例

(1) 配置



交换机1上的配置：

Switch#configure terminal

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport access vlan 2

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport access vlan 2

Switch(config-ge1/2)#interface ge1/3

Switch(config-ge1/3)#switchport access vlan 2

Switch(config-ge1/3)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24

Switch(config-vlan2)#exit

Switch(config)#router vrrp vlan2 1

Switch(config-vrrp)#vrrp ip-address 192.168.1.1

Switch(config-vrrp)#enable vrrp

Switch(config-vrrp)#exit

Switch(config)#router vllp vlan2

Switch(config-vllp)#vlllp port ge1/1

```
Switch(config-vllp)#vllp port ge1/2
Switch(config-vllp)#vllp port ge1/3
Switch(config-vllp)#vllp enable
```

交换机2上的配置：

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 2
Switch(config-ge1/3)#interface vlan2
Switch(config-ge1/3)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.2/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp vlan2 1
Switch(config-vrrp)#vrrp ip-address 192.168.1.1
Switch(config-vrrp)#enable vrrp
Switch(config-vrrp)#exit
Switch(config)#router vllp vlan2
Switch(config-vllp)#vlllp port ge1/1
Switch(config-vllp)#vllp port ge1/2
Switch(config-vllp)#vllp port ge1/3
Switch(config-vllp)#vllp enable
```

(2) 验证

使用下面命令查看 VLLP 信息：

```
show vllp
show vllp <if-name>
show vllp map
```

第17章 配置DHCP RELAY

本章主要包括以下内容：

- DHCP RELAY 介绍
- DHCP RELAY 配置
- DHCP RELAY 配置示例

17.1 DHCP RELAY 介绍

DHCP（动态主机配置协议 Dynamic Host Configuration Protocol）是 BOOTP 的增强版本，为网络上的主机动态配置网络环境，分为服务器端和客户端。服务器端集中管理 IP 网络资料并处理客户端的请求，动态配置客户端的 TCP/IP 环境。DHCP 工作时，至少有一台服务器在网络上，它可以监听网络上主机的 DHCP 请求，并协商 TCP/IP 的参数。其分配有自动和动态两种方式。自动方式，一旦客户端获得 IP 地址后就永久使用该地址。动态方式，客户端获得的 IP 地址有一租约，一旦租约到期就需要释放该 IP；也可以提前续约，或租用其他 IP。动态分配能有效解决实际 IP 不足的问题。

DHCP 的工作过程：

如果客户端是第一次登录网络，它无任何 IP 资料，会广播一 Discover 报文，源地址 0.0.0.0，目的地址 255.255.255.255。若服务器无响应，则根据一定间隔发出四次的 Discover 请求。

服务器接收到 Discover 则选择一空闲 IP 回应客户端 Offer 报文。

若网络上存在多台服务器，客户端会接收到多个 Offer 报文，一般选择最先到达的 Offer，并广播 Request 报文，告诉所有服务器它已接收哪台服务器提供的 IP 地址了。

如果客户端通过 ARP 发现该 IP 已被使用，则发 Decline 报文给服务器，拒绝该 Offer；并重新启动 Discover 过程。

服务器接收到 Request 报文会给客户端发送 Ack 报文确认该租约生效。

若客户端已经申请到 DHCP 的租约，一般无需再使用 Discover 过程了。在租约到期之前使用已经租用的 IP 向服务器发送 Request 续约，服务器会尽量让客户端使用原来的 IP，如果没问题的话，服务器回应 Ack 报文确认。若该 IP 已经被其他客户端使用，则服务器回应 Nack 报文拒绝该续约请求。

客户端可以使用 Release 报文主动解除租约。

工作站在开机时发出 Request 请求；在租约一半时会再发 Request 请求，若无确认仍可使用该 IP；在租约 3/4 时还会发 Request 请求，若这时无确认的话将不能再使用这个 IP 了。

Discover 报文是以广播方式发布的，只能在同一网段内，路由器不会将广播报文扩散出去。当服务器与客户端不在同一网段，客户端还未获得 IP 环境设定，也不知道路由器的位置，这时 Discover 报文是无法到达服务器的。为了解决这个问题，可使用 DHCP relay 的功能，让路由器来中转 DHCP 的协议报文，使得 DHCP 可跨网段运作。

DHCP snooping 主要通过监听 DHCP 协议报文，记录动态获取的 IP 地址与 MAC 地址

关系，记录 MAC 地址与端口关系。ARP 欺骗报文不能修改这样的 ARP 表项，只有 DHCP 动态获取的 IP 信息能够修改。这种方式可以防止 ARP 欺骗。

17.2 DHCP RELAY 配置

DHCP relay 功能多与接口相关，实现 DHCP 跨网段的协议报文转发，在接口模式下进行相关配置。

DHCP-relay 的配置包括：

- 启动接口的 DHCP-relay 功能
- 配置接口对应的 DHCP server
- 启动 DHCP snooping 功能

17.2.1 启动接口的 DHCP-relay 功能

模式：接口配置模式

命令：dhcp relay　　　　在接口上打开 dhcp relay 协议

命令：no dhcp relay　　　关闭接口上 dhcp relay 协议

缺省：不打开 dhcp relay 协议；使用该命令启动接口收发 dhcp 协议报文。

17.2.2 配置接口对应的 DHCP server

模式：接口配置模式

命令：dhcp server <ip-address>

配置服务器 IP，从该接口接收的报文发往指定服务器。

命令：no dhcp server <ip-address>

删除指定服务器

命令：no dhcp server

删除服务器列表

参数：<ip-address>表示服务器的 IP 地址；DHCP-relay 协议主要用于第三层的 DHCP 报文中继，该命令将指定的服务器绑定到相应接口，也即从该接口接收到的协议报文均发往

指定的服务器。这样不同的网段可以分配不同的服务器。

17.2.3 启动 DHCP snooping 功能

模式：全局配置模式

命令：dhcp snooping　　　　　　启动 DHCP snooping 功能

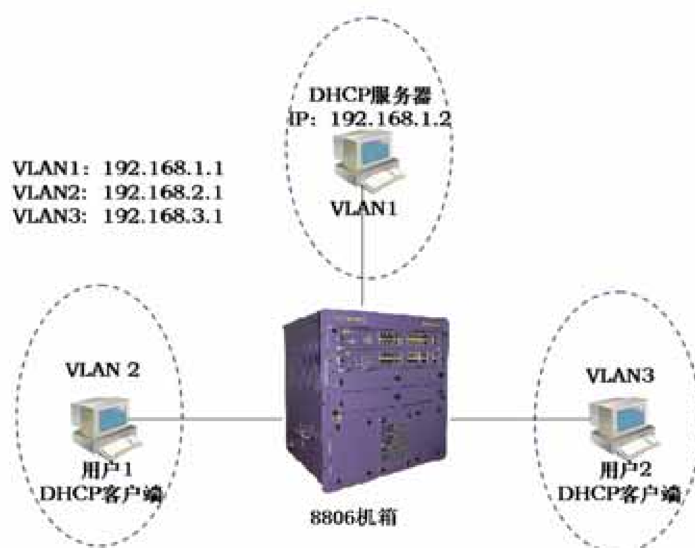
命令：no dhcp snooping　　　　关闭 DHCP snooping 功能

缺省：未启动 DHCP snooping 功能。当打开 DHCP snooping 功能时，从 dhcp 服务器获取的 IP 信息与 MAC 信息会写入 ARP 表，并会绑定申请到 IP 的交换机二层端口。DHCP snooping 功能可以有效防止 ARP 攻击。

17.3 DHCP RELAY 配置示例

(1) 配置

需要对交换机进行DHCP中继转发配置，使交换机能够路由转发用户1和用户2的DHCP请求和DHCP服务器的DHCP回复确认信息。使用户1和用户2能够通过在不同网段的DHCP服务器获得合法IP地址，从而接入网络。



Switch# configure terminal

```
Switch(config)#interface vlan1
Switch(config-vlan1)#ip address 192.168.1.1/24
Switch(config-vlan1)#dhcp relay
Switch(config-vlan1)#interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24
Switch(config-vlan2)#dhcp relay
Switch(config-vlan2)#dhcp server 192.168.1.2
Switch(config-vlan2)#interface vlan3
Switch(config-vlan3)#ip address 192.168.3.1/24
Switch(config-vlan3)#dhcp relay
Switch(config-vlan3)#dhcp server 192.168.1.2
```

(2) 验证

```
show running-config
```

第18章 配置IGMP

本章主要包括以下内容：

- IGMP 介绍
- IGMP 配置
- IGMP 配置示例

18.1 IGMP 介绍

IGMP（Internet 组管理协议 Internet Group Management Protocol）是组播技术的一部分，运行于主机与其直连的组播路由器之间，一方面主机向本地路由器报告其想加入或者离开的组播组，另一方面，组播路由器可以周期性的查询本地主机对于特定组是否处于活动接收状态。IGMP 协议目前有三个版本，版本 1（RFC1112），版本 2（RFC2236），版本 3（RFC3376）。IGMP 基于查询-响应模式，组播路由器使用查询报文周期查询子网中主机是否有想接收的特定组，主机使用报告报文通知本地路由器它想加入或者离开的组播组，即成员关系报告。当主机想加入一个特定组时，并不需要等待周期的查询报文，可以立即发送组成员关系报告给路由器。当路由器查询子网中主机的成员关系时，主机使用抑止机制，延时 1 到 10 秒之间的一个随机值来发送报告报文，当收到其他主机的相同组报告报文则抑止自己的组成员报告发送，从而减少子网中 IGMP 的流量。当子网中有多台路由器时需要比较 IP 地址来选举一台作为查询者，避免子网中过多的 IGMP 查询报文。版本 1 仅支持查询、报告，当组成员离开时，组播路由器只有等待该组信息超时才会停止组播数据流的转发,查询者依赖其它协议选举。版本 2 通过增加离开报文支持组成员的立即离开，当最后一个组成员离开组时，它向路由器发送离开报文，路由器发送特定组查询报文来确定子网中是否还有其他接收主机存在，当在发送了配置的重传次数后依然没有接收到相应组成员关系报文则该组失效，停止转发组播数据流。版本 2 通过离开机制有效的减少了离开延时。版本 2 提供了查询者选举机制，当一般查询报文被子网中其他路由器接收到时，它们各自通过比较自己的 IP 地址选举出 IP 地址最小的担任查询者，并启动一计时器时，每次接收到查询报文时该计时器复位，当计时器终止时，新的选举过程开始。为了调节主机的抑止机制的响应时间，版本 2 的报文中增加了最大响应时间域，查询者可以通过在查询报文中添加该值来控制主机的抑止响应时间，主机接收到查询报文时，使用最大响应时间随机产生一个延时来启动计时器，当在这段延时时间内接收到其他主机的相同组成员关系报文则抑止自己的报告报文。版本 3 支持特定源组播，查询报文分为一般查询、特定组查询、特定组特定源查询三种；报告报文将原来的组地址域扩展为组记录条目，每条组记录包含组地址及其对应的源地址列表，由组记录类型来区分是加入特定源，还是不加入特定源。IGMPv3 与 PIM-SSM 配合，实现特定源组播，由源到接收者直接建立 SPT 而不需要汇聚点 RP。

18.2 IGMP 配置

IGMP 功能多与接口相关，配置各个接口的相应参数及计时器值，在接口模式下进行相关配置。

IGMP 的配置包括：

- 启动接口的 IGMP 功能
- 配置接口的组过滤访问控制列表
- 配置接口离开组过滤的访问控制列表
- 配置接口的特定组查询的次数
- 配置接口的特定组查询间隔
- 配置接口的非查询者计时器时间
- 配置接口的查询计时器间隔
- 配置接口的最大响应时间
- 配置接口的活力参数
- 配置接口的协议版本

18.2.1 启动接口的 IGMP 功能

模式：接口配置模式

命令：ip igmp 在接口上打开 igmp 协议

命令：no ip igmp 关闭接口上 igmp 协议

缺省：不打开 igmp 协议；使用该命令启动接口收发 igmp 协议报文。若全局配置模式下 ip multicast-routing 命令已启动了组播功能支持，那么在接口配置模式下 ip pim sparse-mode 命令启动 pim-sm 协议功能时会自动启动相应接口的 igmp 协议功能。同样，接口配置模式下 no ip pim sparse-mode 命令会自动关闭相应接口的 igmp 协议功能。

18.2.2 配置接口的组过滤访问控制列表

模式：接口配置模式

命令：ip igmp access-group {<acl-id> | <acl-name>}

配置接口的组过滤访问控制列表

命令：no ip igmp access-group

删除该接口的组过滤访问控制列表

参数：<acl-id>表示标准的访问控制列表编号，为整型数 1-99 之间；<acl-name>为标准的访问控制列表名。使用 ACL 可以过滤该接口学习到的组播地址表。ACL 配置细节可参看命令参考手册。

缺省：未配置组过滤 ACL

18.2.3 配置接口离开组过滤的访问控制列表

模式：接口配置模式

命令：ip igmp immediate-leave group-list {<acl-id1> | <acl-id2> | <acl-name>}

配置接口离开组过滤的访问控制列表

命令：no ip igmp immediate-leave

删除该接口的离开组过滤访问控制列表

参数：<acl-id1>表示标准的访问控制列表编号，为整型数 1-99 之间；<acl-id2>为标准的访问控制列表扩展范围的编号，为整型数 1300-1999 之间；<acl-name>为标准的访问控制列表名。使用 ACL 可以过滤该接口接收到版本 2 和版本 3 的离开报文时需要过滤的组播地址。ACL 配置细节参看命令参考手册。

缺省：未配置离开组过滤 ACL

18.2.4 配置接口的特定组查询的次数

模式：接口配置模式

命令：ip igmp last-member-query-count <count>

配置接口特定组查询的次数

命令：no ip igmp last-member-query-count

恢复接口特定组查询次数为缺省值

参数：<count>表示当接收到离开报文时需要发送特定组查询或者特定组特定源查询的次数，为整型数 2-7 之间。在这段时间均未接收到组报告报文才认为该组已无接收主机。

缺省：2

18.2.5 配置接口的特定组查询间隔

模式：接口配置模式

命令：ip igmp last-member-query-interval <interval>

配置接口的特定组查询间隔

命令：no ip igmp last-member-query-interval

恢复接口的特定组查询间隔为缺省值

参数：<interval>表示特定组查询或者特定组特定源查询的时间间隔，为整型数1000-25500 之间，以毫秒为单位；当接收到离开报文时需要发送多次的特定组或者特定组特定源查询，该命令配置多次查询报文的发送间隔。直到多次查询发送完毕均未接收到任何组报告报文才认为该组或者该组该源已无接收主机存在。

缺省：1 秒

18.2.6 配置接口的非查询者计时器时间

模式：接口配置模式

命令：ip igmp querier-timeout <time>

配置接口的非查询者计时器时间

命令：no ip igmp querier-timeout

恢复接口的非查询者计时器时间为缺省值

参数：<time>表示非查询者计时器的终止时间，为整型数 60-300 之间。当子网上存在多台交换机时，需要选举一台作为查询者，负责发送查询报文。网络初始化时，所有的交换机都默认自己是查询者而发送查询报文，当接收到其他交换机的查询报文时，比较彼此的 IP 地址，选举 IP 地址小的为查询者，如果自己不是查询者则启动一计时器，每当接收到查询报文时该计时器复位，若计时器终止则需重新选举查询者。

缺省：255 秒

18.2.7配置接口的查询计时器间隔

模式：接口配置模式

命令：ip igmp query-interval <interval>

配置接口的查询计时器时间间隔

命令：no ip igmp query-interval

恢复接口的查询计时器间隔为缺省值

参数：<interval>表示查询计时器的时间间隔，为整型数 1-18000 之间。当接口启动 IGMP 协议时会相应启动一个查询计时器定时向子网发送查询报文；若有多台交换机则需选举一个查询者，查询者使用该计时器周期性发送查询报文，非查询者关闭该计时器同时启动一个超时计时器，当超时计时器终止时重新选举查询者。

缺省：125 秒

18.2.8 配置接口的最大响应时间

模式：接口配置模式

命令：ip igmp query-max-response-time <time>

配置接口发送查询报文时携带的最大响应时间

命令：no ip igmp query-max-response-time

恢复接口发送查询报文时携带的最大响应时间为缺省值

参数：<time>表示接口发送版本 2 或者版本 3 的查询报文时需携带的最大响应时间值，为整型数 1-240 之间，单位为秒，但是查询报文中的最大响应时间的单位为 0.1 秒。IGMP 使用查询-响应模式获得子网上相应组接收主机的信息，当一台交换机发出查询报文，网络上有多台主机会响应组报告报文，为避免众多 IGMP 报文的拥塞，在查询报文中携带一个最大响应时间值，接收到该查询报文的主机根据这个最大响应时间产生一个随机值，使用随机值延时来发送响应报文，当在这段延时中接收到其他主机发出的一致的组报告报文，那么就抑止自己将要发送的该组的组报告报文，有效的避免了相同时间 IGMP 组报告的冲突。需要注意的是版本 3 的最大响应时间值范围比版本 2 的大，小于 128 的是版本 2 的最大响应时间值范围。

缺省：10 秒

18.2.9 配置接口的活力参数

模式：接口配置模式

命令：ip igmp robustness-variable <value>

配置接口的活力参数

命令：no ip igmp robustness-variable

恢复接口的活力参数为缺省值

参数：<value>表示接口的活力参数，为整型数 2-7 之间。活力参数描述协议的健壮性，当在网络环境比较糟糕的情况下，协议对丢包的适应能力，配置的活力参数值影响到重传次数以及相关计时器的间隔时间。在版本 3 的查询报文中包含 QRV 值，用来同步非查询者本地配置的活力参数。

缺省：2

18.2.10 配置接口的协议版本

模式：接口配置模式

命令：ip igmp version <version>

配置接口的协议版本

命令：no ip igmp versionl

恢复接口的协议版本为缺省值

参数：<version>表示所使用 IGMP 版本号，为整型数 1-3 之间。

缺省：3

18.3 IGMP 配置示例

(1) 配置

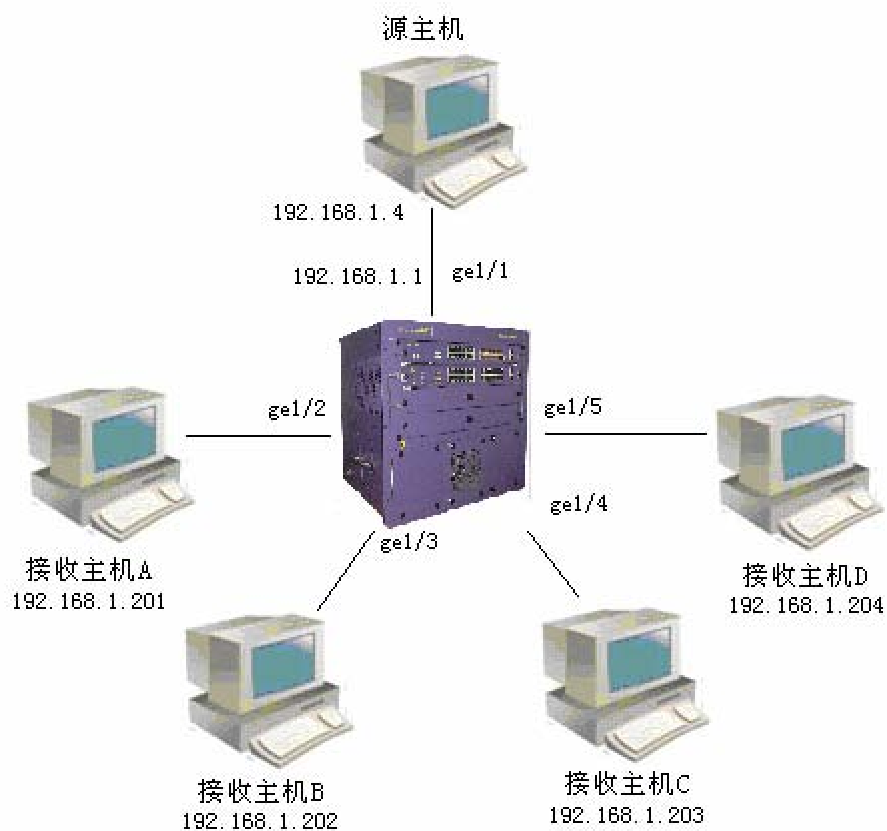
IGMP一般与组播路由协议（eg：PIM-SM）协同工作，见PIM-SM配置示例，启动组播功能（ip multicast-routing）及接口的PIM-SM协议（ip pim sparse-mode）会自动启动相应的IGMP协议，无需单独配置ip igmp命令。当接收端点播组播业务流时，可以查看到相应的IGMP组信息及接口状态。

当源主机与接收主机在同一子网中，组播数据流无需跨网段转发，三层组播路由不必要

时，可单独启动IGMP协议与IGMP snooping来实现子网内组播。注意，需要写三层组播硬件表必须启动PIM-SM协议。

在交换机上：

```
Switch# configure terminal
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#ip igmp
Switch(config-vlan2)#ip pim sparse-mode passive
Switch(config-vlan2)#interface ge1/1
Switch(config-ge1/1)#switch access vlan 2
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switch access vlan 2
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#switch access vlan 2
Switch(config-ge1/3)#interface ge1/4
Switch(config-ge1/4)#switch access vlan 2
Switch(config-ge1/4)#interface ge1/5
Switch(config-ge1/5)#switch access vlan 2
```



(2) 验证

使用下面的命令查看IGMP的信息：

show ip igmp group

show ip igmp interface

第19章 配置PIM-SM

本章主要包括以下内容：

- PIM-SM 介绍
- PIM-SM 配置
- PIM-SM 配置示例

19.1 PIM-SM 介绍

PIM-SM（稀疏模式协议无关组播 Protocol Independent Multicast - Sparse Mode）是组播技术的一部分，用于网络拓扑的发现，是运行于路由器与路由器之间的协议。比较单播点到点之间的传送，组播的点到多点传送致力于建立分布树，使源的数据流能够沿着分布树传送到需要接收的组成员主机。分布树有两种形式，一种是基于源的，每个源每个组一颗分布树，从源到组成员都是最短路径，这种有源树也称为最短路径树 SPT；还有一种是共享一个信息分布点的，一个组的所有源共享一颗树，源的信息需要注册到这个汇聚点(RP:Rendezvous Point)才能够沿着分布树向下传送到接收主机，这种共享树也称为 RPT。PIM-SM 的分布树技术是使用单向共享树的形式，即数据流只能沿从源到接收者的方向流动，而不能反过来。PIM-SM 的设计目标是应用于广域网，即接收者是稀疏分布在网络中的，区别与密集模式的扩散-剪枝方式，PIM-SM 采用加入-剪枝方式来建立共享树，也即接收主机使用显式加入的方式（传统的 IP 多点传送模式，接收端启动成员关系。）。共享树是一个组的所有源共享的分布树，当不同的源需要推送数据流时，源需要注册到汇聚点，再由汇聚点将数据推送到接收者，从源到汇聚点的树是由数据启动的最短路径树。当多个源都注册到汇聚点转发数据流时，汇聚点会成为网络的瓶颈，这时 PIM-SM 允许每个源每个组切换到自己的最短路径树，而不必经过汇聚点。若在一个小型网络中，一个汇聚点足以胜任，若在较大型的网络中，配置多个 RP 来分担任务成为必要，但静态的配置方式不适应网络的动态变化，为此 PIM-SM 提供了 RP 自举机制。在网络中配置多个候选 BSR 及候选 RP，候选 BSR 选举出 BSR，候选 RP 定时将自己的组映射信息发送给 BSR，BSR 收集 RP 信息后整理成自举信息定时在网络中扩散。每台路由器均会保存一份自举信息，当有组成员加入时，查找自举信息找到组对应的 RP 并向 RP 方向发送加入消息，若自举信息中无组对应的 RP 则使用 hash 算法将组映射到某一 RP 并向该 RP 方向发送加入消息。考虑共享网络的情况，PIM-SM 同时提供了 DR 机制及断言机制。指定路由器 DR 应用于加入分布树的过程，断言应用于转发数据流的过程。PIM-SM 因其设计精巧，已成为目前域内组播路由协议的首选；其后又扩展了 PIM-SSM，使用户能够直接从组播源接收业务，这种模型相较与传统的 PIM-SM 具有更突出的优越性。

针对在三层交换机上应用组播协议提出组播安全概念。组播技术可以分为三部分，其一是组播源发现，其二是组播接收者发现，其三是拓扑发现。组播协议一部分是主机与路由器之间的协议，例如 IGMP；一部分是路由器与路由器之间的协议，例如 PIM-SM。组播协议，无论是主机与路由器之间的还是路由器与路由器之间，均以三层接口来描述组播路由的输入输出方向；对于三层交换机来说，如果一个三层接口是一条组播路由的输出接口，那么这个

三层接口对应的 vlan 内所有的二层端口都会是输出端口。这对于下游方向 vlan 内只有一台点播主机来说，vlan 内其他的输出端口是没有必要的。所以 IGMP snooping 协议运行于二层，负责监听从某个端口上来的 IGMP 报文，并记录下来，当有数据流时从该 vlan 输出时，只往有请求的端口发送。也即在三层交换机上需要记录二层端口的信息。同理，在路由器与路由器之间，为维护组播分布树需要发送加入剪枝消息。如果也监听 PIM 协议报文的发送接收端口，那么组播路由表的输出接口也会记录相应的二层端口，当有数据流流经组播树时，只会向 vlan 内有加入消息到达的端口发送而不会向 vlan 内所有的端口发送。监听 PIM 协议报文的二层协议称之为 PIM snooping。有了 IGMP snooping 以及 PIM snooping，运行于路由器的组播路由协议就可以很好的运行于三层交换机，我们看到的组播路由表的条目会是这样显示：

组播源地址 组播组地址 输入接口 输出接口列表 输出端口列表

当有点播数据流时，我们会看到从源到接收主机所经过的组播分布树的分支就是沿着协议报文曾出现的二层端口，而不会是在三层接口对应的 vlan 内泛发。

IGMP snooping 与 PIM snooping 是动态的监听协议，根据协议报文来记录二层端口信息。目前 iSpirit8806 v3.0 版本仅提供实现组播路由条目细化到二层端口的静态配置功能，对于这个功能模块，我们称之为组播安全。它通过静态的配置命令，指定某组播数据流的输出只发给输出接口对应 vlan 内的特定二层端口。在缺省情况下，数据流会向输出接口对应 vlan 内的所有二层端口输出。

19.2 PIM-SM 配置

PIM-SM 协议需在三层组播功能启动后再在各个接口上逐个启动，其相关命令在全局配置模式及接口配置模式下。

PIM-SM 的配置包括：

- 启动组播路由功能
- 配置组播路由表容量
- 配置组播接口 ttl 值
- 启动接口 pim-sm 功能
- 配置接口的被动模式
- 配置接口优先级
- 配置接口 hello 报文不包含 genid 信息
- 配置接口 hello 计时器间隔

- 配置接口上邻居的保持时间
- 配置接口的邻居列表过滤
- 配置单播注册报文的源地址
- 配置注册报文数量限制
- 配置注册时检查 RP 可达
- 配置注册抑止计时器时间值
- 配置注册 KAT 计时器时间值
- 配置注册源地址过滤
- 配置注册报文 cisco 方式的校验和
- 配置静态 RP 地址
- 配置候选 RP
- 配置忽略 RP-set 优先级
- 配置 cisco 方式的 C-RP-Adv 报文
- 配置候选 BSR
- 配置 JP 计时器间隔
- 配置 SPT（最短路径树）切换
- 配置 SSM（特定源组播）
- 配置组播安全

19.2.1 启动组播路由功能

模式：全局配置模式

命令：ip multicast-routing　　　　打开组播路由功能

命令：no ip multicast-routing　　　关闭组播路由功能

缺省：不启动组播路由功能；使用该命令启动组播路由功能及 PIM-SM、IGMP 协议。

19.2.2 配置组播路由表容量

模式：全局配置模式

命令：ip multicast route-limit <limit> [threshold]

配置组播路由表的容量及告警门限值

命令：no ip multicast route-limit

恢复组播路由表的容量及告警门限为缺省值

参数：<limit>表示组播路由表的容量，为整型数 1-2147483647 之间；[threshold]表示组播路由表的告警门限，为整型数 1-2147483647 之间，可选择配置，当组播路由表超过告警门限值时交换机会显示提示信息。

缺省：均为 2147483647

19.2.3 配置组播接口 ttl 值

模式：接口配置模式

命令：ip multicast ttl-threshold < threshold>

配置组播接口的 ttl 值

命令：no ip multicast ttl-threshold

恢复组播接口 ttl 值为无效值

参数：<threshold>表示组播接口的 ttl 值，为整型数 0-255 之间，256 为无效值。该命令配置接口的 ttl 值，用于维护组播路由表的输出接口列表。当配置的 ttl 值在 0-255 之间，该值会传递给实际的组播接口，当该值为 256 时，实际的组播接口使用自己的缺省 ttl 值 1。

缺省：256

19.2.4 启动接口 pim-sm 功能

模式：接口配置模式

命令：ip pim sparse-mode

启动接口 pim-sm 协议

命令：no ip pim sparse-mode

关闭接口 pim-sm 协议

缺省：接口不启动 pim-sm 协议，使用该命令启动接口的 pim-sm 协议功能，收发协议报文，当配置自举时参与 RP 选举。接口启动 pim-sm 会相应启动 igmp 协议，无需再配置 ip igmp 命令。

19.2.5 配置接口的被动模式

模式：接口配置模式

命令：ip pim sparse-mode passive

配置接口为被动模式

命令：no ip pim sparse-mode passive

取消接口的被动模式恢复为活动状态

缺省：不启动 pim-sm 协议，当使用 ip pim sparse-mode 命令启动接口的 pim-sm 功能时，为活动状态，接口正常收发协议报文；当配置为被动模式，接口不发送协议报文，不参与注册过程，不参与 RP 选举过程，只静静的监听协议报文。

19.2.6 配置接口优先级

模式：接口配置模式

命令：ip pim dr-priority <priority>

配置接口参与 DR 选举的优先级

命令：no ip pim dr-priority [priority]

恢复接口优先级为缺省值

参数：<priority>表示接口参与 DR 选举的优先级，为整型数 0-4294967294 之间。当共享网络上有多台交换机，通过 hello 协议来选举一台担任 DR，负责向上游发送加入剪枝消息。DR 的选举先比较优先级，选择优先级高的；优先级相同，选择 IP 地址大的作为 DR。

缺省：1

19.2.7 配置接口 hello 报文不包含 genid 信息

模式：接口配置模式

命令：ip pim exclude-genid

配置接口 hello 报文不包含 genid 域

命令：no ip pim exclude-genid

恢复接口 hello 报文 genid 域配置为缺省配置

缺省：包含 genid 域；hello 报文选项列表中类型 20 为 generation id 选项值，genid 为接口启动时随机产生的一个无符号 32 位值，用于快速识别是否有邻居重启，减少因路由器重启需要重新学习 rp-set 信息及加入剪枝状态花费的延时。交换机保留 hello 报文中的 genid 值，接收到新的 hello 报文会更新这个值，若 genid 发生变化则认为邻居重启，需要及时的告知其相关信息，而不是等待计时器终止时才自己学习，减少了网络变化时收敛的时间。

19.2.8 配置接口 hello 计时器间隔

模式：接口配置模式

命令：ip pim hello-interval <interval>

配置接口的 hello 计时器间隔

命令：no ip pim hello-interval

恢复接口 hello 计时器间隔为缺省值

参数：<interval>表示接口发送 hello 报文的间隔，为整型数 1-65535 之间。hello 计时器间隔的设置会影响 holdtime 值，该值是 hello 间隔的 3.5 倍，当该值为未配置或者配置的值小于 hello-interval 时需要根据 hello-interval 来计算。

缺省：30 秒

19.2.9 配置接口上邻居的保持时间

模式：接口配置模式

命令：ip pim hello-holdtime <value>

配置发送 hello 报文的邻居的保持时间

命令：no ip pim hello-holdtime

恢复邻居保持时间为缺省值

参数：<value>表示邻居的存活时间，为整型数 1-65535 之间；若在 hold time 时间内未接收到 hello 报文则认为邻居已经不再存在。配置该值时必须大于 hello interval 的值，若小于 hello interval 值，则会使用 hello interval 的 3.5 倍作为 hold time 的值。

缺省：105 秒（hello interval 的 3.5 倍）

19.2.10 配置接口的邻居列表过滤

模式：接口配置模式

命令：ip pim neighbor-filter {<acl-id> | <acl-name>}

配置接口的邻居列表过滤 ACL

命令：no ip pim neighbor-filter {<acl-id> | <acl-name>}

取消接口的邻居列表过滤

参数：<acl-id>表示标准访问控制列表的编号，为整型数 1-99 之间；<acl-name>表示标准的访问控制列表名。使用 ACL 过滤接口的邻居列表，当邻居被 ACL 过滤了则从接口的邻居列表中删除。ACL 配置细节参看命令参考手册。

缺省：未配置邻居过滤 ACL

19.2.11 配置单播注册报文的源地址

模式：全局配置模式

命令：ip pim register-source {<ip> | <if-name>}

配置单播注册报文的源地址或者接口名

命令：no pim register-source

取消注册报文源地址的配置

参数：<ip>表示单播注册报文的源地址，为点分十进制格式；<if-name>表示单播注册报文的源接口名，为三层接口名（eg：vlan2）。该命令用于指定注册报文的源地址。

缺省：不配置注册报文的源地址，使用接收到数据包的接口地址。

19.2.12 配置注册报文数量限制

模式：全局配置模式

命令：ip pim register-rate-limit <limit>

配置 1 秒内接收的注册报文数量门限

命令：no ip pim register-rate-limit

取消注册报文数量限制检查

参数：<limit>表示 1 秒内可接收的注册报文数量最大值，为整型数 1-65535 之间。注册报文实际封装了数据包在内，当源注册时，会有较大的数据流冲击源的第一跳路由器，这时可限制上 pim-sm 协议的数据流，避免路由器较大的负担。因为 pim-sm 只是需要数据流来触发源到 RP 的 SPT 建立，所以可以使用限制机制。当限制数据流量时，检查 1 秒内的数据包数量，若两个数据包到达间隔超过 1 秒则不限制。

缺省：不配置注册报文数量限制（门限值为 0）

19.2.13 配置注册时检查 RP 可达

模式：全局配置模式

命令：ip pim register-rp-reachability

配置注册时检查 RP 是否可达

命令：no ip pim register-rp-reachability

配置注册时无需检查 RP 是否可达

缺省：注册时无需检查 RP 是否可达

19.2.14 配置注册抑止计时器时间值

模式：全局配置模式

命令：ip pim register-suppression <value>

配置注册抑止计时器时间值

命令：no ip pim register-suppression

恢复注册抑止计时器时间为缺省值

参数：<value>表示注册抑止计时器的时间值，为整型数 1-65535 之间。

缺省：60 秒

19.2.15 配置注册 KAT 计时器时间值

模式：全局配置模式

命令：ip pim rp-register-kat <value>

配置 RP 上注册创建的(S,G)条目的 kat 计时器时间

命令：no ip pim rp-register-kat

恢复(S,G)的 kat 计时器时间为缺省值

参数：<value>表示 RP 上源注册创建的(S,G)条目的 kat 计时器的时间值，为整型数 1-65535 之间。

缺省：185 秒（3 * register-suppression + register-probe）

19.2.16 配置注册源地址过滤

模式：全局配置模式

命令：ip pim accept-register list {<acl-id1> | <acl-id2> | <acl-name>}

配置注册报文的源过滤列表

命令：no ip pim accept-register

取消注册报文的源过滤列表

参数：<acl-id1>表示扩展的访问控制列表编号，为整型数 100-199 之间；<acl-id2>表示扩展的访问控制列表扩展部分编号，为整型数 2000-2699 之间；<acl-name>表示访问控制列表名。使用访问控制列表可以过滤注册到 RP 的源地址，若 RP 上源地址被 ACL 过滤，则相应的(S,G)条目从组播路由表删除。ACL 配置细节参看命令参考手册。

缺省：未配置注册源的 ACL

19.2.17 配置注册报文 cisco 方式的校验和

模式：全局配置模式

命令：ip pim cisco-register-checksum [group-list {<acl-id1> | <acl-id2> | <acl-name>}]

配置注册报文校验和为 cisco 方式

命令：no ip pim cisco-register-checksum [group-list {<acl-id1> | <acl-id2> | <acl-name>}]

取消注册报文校验和为 cisco 方式

参数：<acl-id1>表示标准访问控制列表的编号，为整型数 1-99 之间；<acl-id2>表示标准访问控制列表扩展部分的编号，为整型数 1300-1999 之间；<acl-name>表示标准访问控制列表名。 Cisco 方式的校验和为计算整个注册报文的校验和（包含数据包部分），而一般

的注册报文的校验和只包含 pim-sm 协议报文头及注册报文的头。若配置了访问控制列表，那么在发送注册报文时需要使用 ACL 过滤相应的组地址，通过 ACL 的可以使用 cisco 方式的校验和，通不过 ACL 的使用一般方式的校验和。

缺省：不配置 cisco 方式的校验和

19.2.18 配置静态 RP 地址

模式：全局配置模式

命令：ip pim rp-address <ip> [<acl-id1> | <acl-id2> | <acl-name>]

配置静态 RP

命令：no ip pim rp-address <ip> [<acl-id1> | <acl-id2> | <acl-name>]

取消静态 RP 配置

参数：<ip>表示静态 RP 的地址，为点分十进制格式；<acl-id1>表示标准访问控制列表的编号，为整型数 1-99 之间；<acl-id2>表示标准访问控制列表扩展部分的编号，为整型数 1300-1999 之间；<acl-name>表示标准访问控制列表名。

缺省：不配置静态 RP

19.2.19 配置候选 RP

模式：全局配置模式

命令：ip pim rp-candidate <if-name> [group-list {<acl-id> | <acl-name>} | interval <value1> | priority <value2>]

配置接口为 C-RP

命令：no ip pim rp-candidate [if-name]

取消接口 C-RP 属性

参数：<if-name>表示配置为 C-RP 的接口名，为三层接口名（eg：vlan2）；<acl-id>表示标准访问控制列表的编号，为整型数 1-99 之间；<acl-name>表示标准访问控制列表名；<value1>表示 C-RP 周期性单播 C-RP-adv 报文到 BSR 的时间间隔，为整型数 1-16383 之间；<value2>表示 C-RP 的优先级，为整型数 0-255 之间，包含在自举信息中在域内泛洪，用于组对应 RP 的选择。

缺省：value1 缺省为 60 秒；value2 缺省为 192。

19.2.20 配置忽略 RP-set 优先级

模式：全局配置模式

命令：ip pim ignore-rp-set-priority

配置在 RP-set 中查找 RP 时忽略优先级使用 hash 算法映射

命令：no ip pim ignore-rp-set-priority

配置在 RP-set 中查找 RP 使用优先级

缺省：在 RP-set 中查找 RP 使用优先级顺序

19.2.21 配置 cisco 方式的 C-RP-Adv 报文

模式：全局配置模式

命令：ip pim crp-cisco-prefix

配置 C-RP-Adv 报文为 cisco-BSR 可接收的格式

命令：no ip pim crp-cisco-prefix

配置 C-RP-Adv 报文为标准 RFC 格式

缺省：C-RP-Adv 报文为标准 RFC 格式。Cisco-BSR 不接收 C-RP-Adv 报文 prefix-cnt 域为 0 的协议报文，缺省若无组地址，prefix-cnt 域为 1，填写一条 224.0.0.0 的组地址。标准 RFC 缺省若无组地址，prefix-cnt 域为 0。该命令兼容 BSR 是 cisco 的路由器，需要发送 cisco-BSR 能够识别的 C-RP-Adv 报文。

19.2.22 配置候选 BSR

模式：全局配置模式

命令：ip pim bsr-candidate <if-name> [<hash-mask-len> | <priority>]

配置候选 BSR 的接口、优先级及 hash 计算的掩码长度

命令：no ip pim bsr-candidate [if-name]

取消接口的候选 BSR 身份

参数：<if-name>表示担任候选 BSR 的接口名，为三层接口名（eg：vlan2）；<hash-mash-len>表示 hash 算法中掩码长度，为整型数 0-32 之间；<priority>表示候选 BSR

参与 BSR 选举时的优先级，为整型数 0-255 之间。当候选 BSR 当选为 BSR 时，其 hash-mask-len 及 priority 均在自举报文中传递。

缺省：priority 缺省值为 0；hash-mask-len 缺省值为 10。

19.2.23 配置 JP 计时器间隔

模式：全局配置模式

命令：ip pim jp-timer <time>

配置上游的加入剪枝计时器间隔

命令：no ip pim jp-timer [time]

恢复上游的加入剪枝计时器间隔为缺省时间

参数：<time>表示交换机向上游周期性发送加入剪枝报文的时间间隔，为整型数 1-65535 之间。交换机通过 JP 计时器来维护组播分布树的转发状态。加入剪枝状态的保持时间为 3.5 倍的 JP 计时器间隔，保持时间包含在加入剪枝报文中。

缺省：60 秒

19.2.24 配置 SPT 切换

模式：全局配置模式

命令：ip pim spt-threshold [group-list <acl-id1> | <acl-id2> | <acl-name>]

配置 SPT 切换

命令：no ip pim spt-threshold [group-list <acl-id1> | <acl-id2> | <acl-name>]

取消 SPT 切换

参数：<acl-id1>表示标准访问控制列表的编号，为整型数 1-99 之间；<acl-id2>表示标准访问控制列表扩展部分的编号，为整型数 1300-1999 之间；<acl-name>表示标准访问控制列表名。当配置了 SPT 切换，可以使用访问控制列表过滤组播路由表的(*,G)条目，通过 ACL 的可以配置 SPT 切换，通不过的不可以配置 SPT 切换。

缺省：未配置 SPT 切换

19.2.25 配置 SSM

模式：全局配置模式

命令：ip pim ssm {default | range {<acl-id> | <acl-name>}}

配置 SSM（特定源组播）

命令：no ip pim ssm

取消 SSM

参数：<acl-id>表示标准访问控制列表的编号，为整型数 1-99 之间；<acl-name>表示标准访问控制列表名。

缺省：不配置 SSM

19.2.26 配置组播安全

模式：全局配置模式

命令：ip mroute <src-addr> <grp-addr> <iif-name> <oif-name> remove <if-name>

对于某组播路由(S,G)某输出接口对应 vlan 内特定二层端口不转发数据流

命令：ip mroute <src-addr> <grp-addr> <iif-name> <oif-name> add <if-name>

将某组播路由(S,G)的某一输出端口添加回其所在 vlan 对应的输出接口中

参数： src-addr 表示组播路由(S,G)的组播源地址

grp-addr 表示组播路由(S,G)的组播组地址

iif-name 表示组播路由(S,G)的输入接口

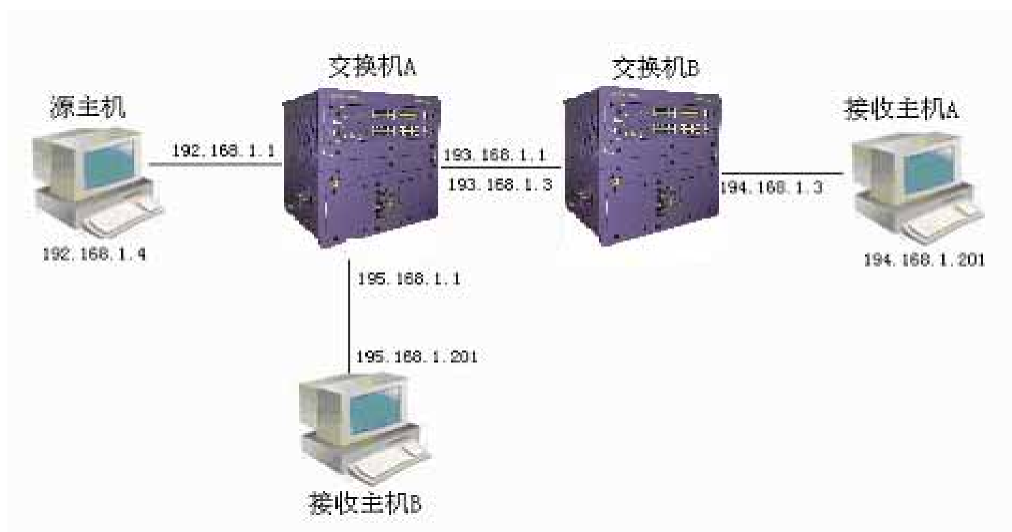
oif-name 表示组播路由(S,G)的输出接口

if-name 表示组播路由(S,G)的输出接口对应 vlan 内的二层端口，remove 命令将这个二层端口从输出接口所在的 vlan 内屏蔽出去，也即从该输出接口转发出的数据流不会从该二层端口转发出去。add 命令将这个二层端口加回输出接口所在的 vlan 内，也即从该输出接口转发出的数据流会从该二层端口转发出去。

缺省：输出接口对应的 vlan 内所有的二层端口都会转发组播数据流

19.3 PIM-SM 配置示例

(1) 配置



启动PIM-SM协议，使接收主机能够从源主机接收组播数据流。

在交换机A上：

```
Switch#configure terminal
Switch(config)#ip multicast-routing
Switch(config)#ip pim rp-address 193.168.1.3
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#ip pim sparse-mode
Switch(config-vlan2)#interface vlan3
Switch(config-vlan3)#ip address 193.168.1.1/24
Switch(config-vlan3)#ip pim sparse-mode
Switch(config-vlan3)#interface vlan5
Switch(config-vlan5)#ip address 195.168.1.1/24
Switch(config-vlan5)#ip pim sparse-mode
```

在交换机B上：

```
Switch#configure terminal
Switch(config)#ip multicast-routing
Switch(config)#ip pim rp-address 193.168.1.3
Switch(config)#interface vlan3
Switch(config-vlan3)#ip address 193.168.1.3/24
```

Switch(config-vlan3)#ip pim sparse-mode
Switch(config-vlan3)#interface vlan4
Switch(config-vlan4)#ip address 194.168.1.3/24
Switch(config-vlan4)#ip pim sparse-mode

(2) 验证

使用下面命令查看 PIM-SM 信息：

show ip pim sparse-mode interface
show ip pim sparse-mode neighbor
show ip pim sparse-mode local-members
show ip pim sparse-mode mroute
show ip pim sparse-mode rp mapping

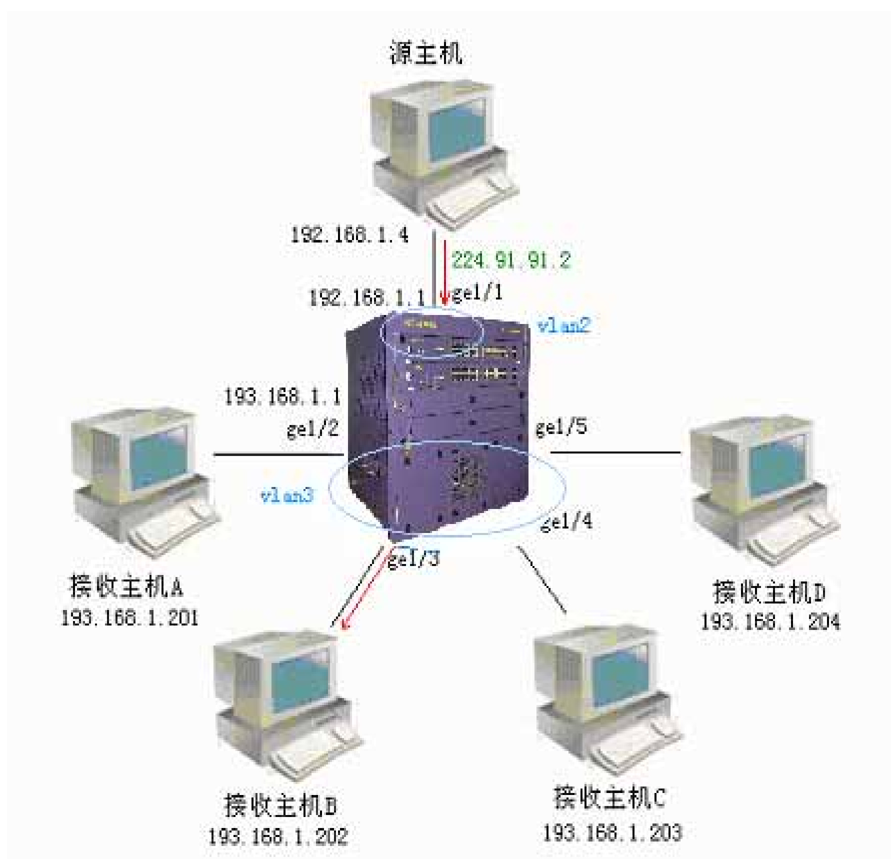
(3) 配置组播安全

组播安全功能模块是运行在组播路由协议之上的，先启动组播路由协议，再根据具体的某一条组播路由来配置其输出接口的二层端口转发状态。如下图所示，vlan2连接组播源192.168.1.4；vlan3内有四台主机，分别连接端口ge1/2、ge1/3、ge1/4和ge1/5；由图中红色箭头所示，只有主机193.168.202点播了组播组224.91.91.2的节目，其他三台主机并没有参与组播点播，那么从这三个二层端口转发出的数据流是没有必要的，通过配置静态组播命令将ge1/2、ge1/4、ge1/5屏蔽出去。

在交换机上：

Switch#configure terminal
Switch(config)#ip multicast-routing
Switch(config)#ip pim rp-address 193.168.1.1
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#ip pim sparse-mode
Switch(config-vlan2)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#interface vlan3
Switch(config-vlan3)#ip address 193.168.1.1/24
Switch(config-vlan3)#ip pim sparse-mode
Switch(config-vlan3)#interface ge1/2
Switch(config-ge1/2)#switchport access vlan 3

```
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 3
Switch(config-ge1/3)#interface ge1/4
Switch(config-ge1/4)#switchport access vlan 3
Switch(config-ge1/4)#interface ge1/5
Switch(config-ge1/5)#switchport access vlan 3
Switch(config-ge1/5)#exit
Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/2
Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/4
Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/5
```



第20章 配置SNMP

ISpirit8806交换机提供了SNMP对交换机进行远程管理。本章描述如何配置SNMP，主要包括以下内容：

本章主要包括以下内容：

- SNMP 介绍
- SNMP 配置
- SNMP 配置示例

20.1 SNMP 介绍

SNMP 是简单网络管理协议，是目前使用最广泛的网络管理协议，它具有五大功能：故障管理，计费管理，配置管理，性能管理，安全管理。它提供网管应用软件和网管代理（agent）之间通信的信息格式。

SNMP 网络管理协议有四大要素：管理工作站，管理代理，管理信息库，网络管理协议。管理代理在交换机上，是管理工作站访问交换机的服务端，管理工作站访问网管代理的信息以 MIB 的形式组织，形成管理信息库。

SNMP 有三大操作：GET 操作，SET 操作，TRAP 操作。GET 操作使管理工作站能够获取代理中对象的值。SET 操作使管理工作站能够设置代理中对象的值。TRAP 操作使代理能够向管理工作站通告事件。

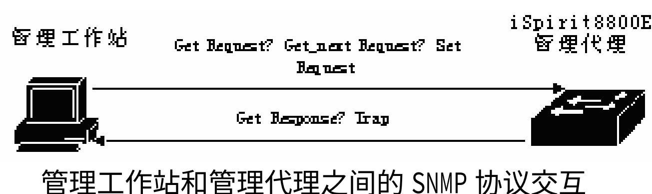
TRAP 消息是当交换机发生事件时主动发给管理工作站的，这些消息包括冷启动，热启动，端口的 link up、link down，共用体名认证失败，STP 的状态切换，模块的上线或下线的通知等。

目前 SNMP 有三个版本：SNMPV1，SNMPV2，SNMPV3 个，后面的版本是前面的升级版，功能进行了增强，安全性得到提高。iSpirit8806 交换机支持所有的三个 SNMP 版本，可以对三个版本的 SNMP 协议包进行解析。当发送 TRAP 消息时，可以使用 SNMPV1，SNMPV2 和 SNMPV3 中的任何一个版本发送。

iSpirit8806 交换机支持 RFC，BRIDGE 和私有的 MIB 对象，通过 SNMP 可以完全管理交换机。下面列出了 iSpirit8806 交换机支持的一些 MIB：RFC 1213 ，RFC 1493 ，RFC 1724 ,RFC 1850 ,RFC 1907 ,RFC 2233 ,RFC 2571,RFC 2572 ,RFC 2573，RFC 2574 ，RFC 2575 ，

RFC 2674 等共有的 MIB.

如图是管理工作站与管理代理之间的 SNMP 协议交互的例子。管理工作站可以通过发送 Get Request、GetNext Request、GetBulk Request 和 Set Request 的 SNMP 消息访问交换机管理代理，获取或设置交换机的 MIB 对象的值，交换机管理代理回送 Get Response 的 SNMP 消息给管理工作站。当交换机上发生了一些事件时，交换机的管理代理主动发送 SNMP TRAP 消息给管理工作站。



管理工作站和管理代理之间的 SNMP 协议交互

20.2 SNMP 配置

SNMP 配置包括交换机的 community 配置，TRAP 工作站，snmp 系统信息的配置和 snmpV3 的 engine id，user 以及 group 的配置。iSpirit8806 交换机缺省有一个只读的共用体，共用体名为 public，交换机最多可以配置 8 个共用体。iSpirit8806 交换机缺省没有配置 TRAP 工作站。iSpirit8806 交换机缺省有一个 local engine id，交换机可以修改该 local engine id。iSpirit8806 交换机缺省有一个 user name：initialnone，该用户名属于非鉴别非加密用户名，交换机可以配置多个不同级别的用户名。iSpirit8806 交换机缺省有一个 group name：initial，交换机可以根据不同用户名对应配置不同的 group name。

SNMP 的命令如下表：

命令	描述	CLI模式
snmp community <community-name> {ro | rw}	配置访问网管的共用体名称，这是一个交互式命令。配置时用户可以根据提示输入需要的创建的共用体名称，和读/写权限。	全局配置模式
no snmp community <community-name>	删除指定的SNMP共用体名。	全局配置模式
snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}	添加或修改snmp trap的发送目标。这是一个交互式命令。notify name是唯一的，如果修改了已经存在的name，则可以修改这个trap发送目标项。host是发送trap的目标地址；version是以snmpV1，snmpV2c还是snmpV3的方式发送。这个命令缺省配置了	全局配置模式

	目标端口是162。	
no snmp trap <notify-name>	删除指定的SNMP trap。	全局配置模式
snmp system information <contact | location | name> <information-string>	配置系统信息，可配置的系统信息包括：contact，location和name。	全局配置模式
no snmp system information <contact | location | name >	删除某个系统配置信息。	全局配置模式
snmp engine-id local <engine-id-octet-string>	配置SNMP版本3所使用的engine ID。该ID为一个24位的十六进制数；且输入不足24位时，自动用0补齐。	全局配置模式
snmp user <user-name> <group-name> v3 [auth {md5 | sha} <auth-key>]	snmp user命令是设置snmpv3本地的engine ID所对应的某个用户名。及该用户名对应的组名，如果该用户名支持鉴别，则需设置鉴别协议（md5或sha）及相应的鉴别密码。	全局配置模式
no snmp user <user-name> <group-name> v3	删除snmpv3本地的engine ID所对应的某个用户名。	全局配置模式
snmp group <group-name> v3 {auth | noauth} [notify <notify view name> | write <write view name> | read <read view name>]	snmp group命令是设置某个组名，安全级别是（auth或noauth），安全模型（v3）所指定的通知、可写或可读的视图。	全局配置模式
no snmp group <group-name> v3 {auth | noauth}	删除某个组名，安全级别是（auth或noauth），安全模型（v3）所指定的视图。	全局配置模式
show snmp community	显示目前所有的公用体名及相应的读写权限信息。	普通模式/特权模式
show snmp trap	显示目前所有的trap名及相应的trap发送的目标IP地址	普通模式/特权模式

	和版本信息。	
show snmp system information	显示SNMP设置的系统信息。	普通模式/特权模式
show snmp engine-id	显示SNMPV3的local engine-id。	普通模式/特权模式
show snmp user [specify name of user]	显示snmpv3本地的engine ID所对应的某个用户名信息。包括该用户名对应的组名以及该用户名支持的鉴别和加密信息。	普通模式/特权模式
show snmp group	显示所有的组名，安全级别（auth或noauth），安全模型（v3）所指定的通知、可写或可读的视图信息。	普通模式/特权模式

20.3 SNMP 配置示例

20.3.1 配置

配置一个名为 private 的共用体名称操作权限为读写。

配置一个名为 test 的 SNMP trap 且发送目的 IP 为 192.168.0.10；使用的 SNMP 版本为 1。

配置系统的 contact 的具体内容为：E-mail:networks@lenovo.com。

配置系统的 location 具体内容为：ShennanRoad,Shenzhen,China。

配置系统的 name 具体内容为：iSpirit8806。

设置某支持 md5 鉴别的用户名 initialmd5，组名为 initia，鉴别密码为 047b473f93211a17813ce5fff290066b。

设置组名为 initial，安全级别是（auth），安全模型（v3）所指定的通知，可写或可读的视图名分别为 internet，internet，internet。

交换机的配置如下：

Switch#config t

Switch(config)#snmp community private rw

Switch(config)#snmp system information contact E-mail:networks@lenovo.com

Switch(config)#snmp system information location ShennanRoad,Shenzhen,China

Switch(config)#snmp system information name iSpirit8806

Switch(config)# snmp user initialmd5 initial v3 auth md5 047b473f93211a17813ce5fff290066b

Switch(config)# snmp group initial v3 auth read internet write internet notify internet

第21章 配置系统日志

本章主要包括以下内容：

- 系统日志介绍
- 系统日志配置

21.1 系统日志介绍

系统日志模块是交换机的一个重要组成部分，它用来记录整个系统的运行情况，异常行为及用户的操作行为，帮助管理员及时了解和监控系统的工作情况。系统日志模块管理系统的所有来源于正在运行的各个模块的日志信息，对日志信息进行收集，分类，存储和显示输出。

在日志系统中，还有一个重要的 debugging 的功能。系统日志与 debugging 配合，可以帮助管理员或其他技术人员监控网络的运行情况，调试和诊断网络中出现的故障。管理员可以方便地选择需要调试的内容，通过观察 debugging 输出的日志信息，来定位和解决设备或网络的故障。

本节主要包括以下内容：

- 日志信息的格式
- 日志的存储
- 日志的显示
- debugging 工具

21.1.1 日志信息的格式

日志信息的格式如下：

时间戳 优先级: 模块名: 日志内容

时间戳与优先级之间有一个空格，优先级与模块名之间有一个冒号和一个空格，模块名与日志内容之间有一个冒号和一个空格。

日志信息的格式的例子如下：

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge2/2

在这条日志信息中，时间戳是 2006/05/20 13:56:34；优先级是 Warning；模块名是 MSTP；日志内容是 Port up notification received for port ge2/2。

1）时间戳

时间戳的格式：年/月/日 小时:分:秒。

小时采用的是 24 小时制的，从 0 到 23。

时间戳记录的是这条日志信息产生的时间，使用的是交换机的系统时间。系统时间在交换机出厂时已经设置，管理员也可以修改，设备断电后系统时间依然能够运行。

2）优先级

优先级记录这条日志信息的重要程度，根据日志信息的重要程度把日志信息分为四级，优先级从高到低的顺序为：Critical，Warning，Informational 和 Debugging。优先级的描述如下表：

优先级	描述
Critical	严重的错误
Warning	一般的错误，警告，非常重要的提示
Informational	重要的提示，一般的提示，诊断信息
Debugging	调试信息

3）模块名

模块名记录这条日志信息产生的模块，下表列出了一些主要的产生日志信息的模块：

模块名	描述
CLI	命令行接口模块
MSTP	多实例生成树协议模块
VLAN	VLAN 功能模块
OSPF	OSPF 协议模块
RIP	RIP 协议模块
ARP	ARP 协议模块
IP	IP 协议模块
ICMP	ICMP 协议模块
UDP	UDP 协议模块
TCP	TCP 协议模块
VRRP	VRRP 协议模块
DHCP-relay	DHCP RELAY 协议模块

IGMP	IGMP 协议模块
PIM-SM	PIM-SM 协议模块
brd_mgr	模块管理模块

4）日志内容

日志内容是一个短语或句子，代表该日志信息的内容大意，管理员通过阅读日志内容可以知道系统发生了什么事情。

21.1.2 日志的存储

日志的存储一般有三种方式，分别是：

- 日志存储在内存中。
- 日志存储到 NVM 中。
- 日志存储到服务器中。

根据日志的优先级在内存中存在四张日志表，每张表存放一种优先级的日志信息，也就是根据日志的优先级把日志分成四类，每类日志存在一个单独的日志表中。每张日志表都有 1K 个条目，可以存放 1K 条日志信息，当日志表满时后面的日志覆盖时间最久的日志信息。这种存储方式有一个问题，当系统重新启动后这些日志信息都没有了，管理员在系统崩溃的时候没法看到日志信息，没法定位问题。

对于重要的日志信息，如优先级为 Critical 和 Warning 的日志信息，可以把这些日志信息存储到系统的 NVM 中。这种存储方式在系统重启后，NVM 中的日志信息还能够被保留，便于管理员在系统崩溃时定位问题。但这种存储方式有一个问题是由于 NVM 的容量限制，在 NVM 中存储的日志信息条目非常有限。

还有一种比较好的方式是把日志信息存储到服务器中，使用 SYSLOG 协议可以实现，日志信息可以实时地发送到服务器上，服务器保存这些日志信息并显示在一个界面上。这种存储方式不仅便于用户查看日志信息，而且容量巨大，可以把大量的日志信息都存储在服务器上。

目前系统只支持把日志信息存储到内存中，不支持把日志信息存储到 NVM 或服务器中。

21.1.3 日志的显示

日志的显示有两种方式：手工显示和实时显示。手工显示就是用户通过输入命令的方式把日志信息显示出来，实时显示就是当产生日志信息时，日志信息直接输出到终端上，用户可以及时看到。

对于手工显示的方式，用户可以查看所有的日志信息，也可以查看一个优先级的日志信息。日志信息的显示顺序是最后产生的日志信息放在最前面，这样用户可以先看到交换机最近的运行状态。

对于实时显示的方式，用户必须打开终端实时显示开关。如果开关是打开的，产生的日志信息不仅写入到日志表中，而且日志信息也输出到终端上，如果开关是关闭的，则日志信息不会实时显示在终端上。系统目前只能把日志信息实时输出到 Console 终端上，不支持把日志信息输出到 Telnet 终端上。

21.1.4 debugging 工具

debugging 是用于设备和网络的诊断工具，对系统和模块的数据包收发，模块的状态机变化等进行跟踪，可以让管理员了解和监控系统和模块的运行过程，如果网络或设备出现了异常情况，可以通过 debugging 工具跟踪到。

debugging 工具提供了丰富的开关，通过控制这些开关，管理员可以跟踪自己感兴趣的内容。当设备或网络出现异常时，管理员可以打开与此异常相关的 debugging 开关，通过跟踪系统和模块的执行过程找到问题所在。

当某个 debugging 开关打开时，系统会产生相关的日志信息，这些日志信息会写到相应的日志表中。一般情况下，debugging 产生的日志信息的优先级是 Informational。当终端实时显示开关打开时，这些日志信息会实时输出到终端上。当 debugging 开关关闭时，系统不会产生相关的日志信息。

21.2 系统日志配置

系统日志配置包括以下内容：

- 配置终端实时显示开关
- 查看日志信息
- 配置 debugging 开关
- 查看 debugging 信息

21.2.1 配置终端实时显示开关

缺省情况下终端实时显示开关是关闭的，系统产生的日志信息都写入到日志表中，但不会实时显示在终端上。系统中也有些日志信息是不受此开关的限制，如模块上线和下线信息，这些日志信息总会实时输出到 Console 终端上。

终端实时显示开关是与系统日志的优先级对应的，如果某个优先级的终端实时显示开关打开，则该优先级的日志信息会实时显示在终端上，如果某个优先级的终端实时显示开关没有打开，则该优先级的日志信息不会实时显示在终端上。

交换机目前只能在 Console 终端上实时显示日志信息，不能在 Telnet 终端上实时显示日志信息。

当用户使用 write 命令把系统当前配置存储到配置文件时，终端实时显示开关的配置不会存储到系统的配置文件中，当系统重启后这些配置将丢失，需要重新配置。

配置终端实时显示开关的命令如下表：

命令	描述	CLI 模式
log display [critical | warning | informational | debugging]	打开终端实时显示开关。如果不输入参数，打开所有优先级的终端实时显示开关，如果输入其中一个参数，打开指定的优先级的终端实时显示开关。	特权模式
no log display [critical | warning | informational | debugging]	关闭终端实时显示开关。如果不输入参数，关闭所有优先级的终端实时显示开关，如果输入其中一个参数，关闭指定的优先级的终端实时显示	特权模式

	开关。	

21.2.2 查看日志信息

查看日志信息的命令如下表：

命令	描述	CLI 模式
show log display	显示所有优先级的终端实时显示开关的配置。	普通模式，特权模式
show log [critical | warning | informational | debugging]	显示日志表中的日志信息。如果不输入参数，显示所有的日志表的日志信息，如果输入其中的一个参数，显示指定的优先级的日志表的日志信息。	普通模式，特权模式

21.2.3 配置 debugging 开关

系统提供了丰富的 debugging 开关，涉及到多个模块，这里只列出每个模块的示意的命令，关于命令的完整格式参见命令手册。

当用户使用 write 命令把系统当前配置存储到配置文件时，debugging 开关的配置不会存储到系统的配置文件中，当系统重启后这些配置将丢失，需要重新配置。

配置 debugging 开关的示意命令如下：

命令	描述	CLI 模式
debug ip …	打开系统收发 IP 包的相关的 debugging 开关。	特权模式
no debug ip …	关闭系统收发 IP 包的相关的 debugging 开关。	特权模式
debug ip icmp …	打开系统收发 ICMP 包的相	特权模式

	关的 debugging 开关。	
no debug ip icmp …	关闭系统收发 ICMP 包的相关的 debugging 开关。	特权模式
debug ip arp …	打开系统收发 ARP 包的相关的 debugging 开关。	特权模式
no debug ip arp …	关闭系统收发 ARP 包的相关的 debugging 开关。	特权模式
debug ip udp …	打开系统收发 UDP 包的相关的 debugging 开关。	特权模式
no debug ip udp …	关闭系统收发 UDP 包的相关的 debugging 开关。	特权模式
debug ip tcp …	打开系统收发 TCP 包的相关的 debugging 开关。	特权模式
no debug ip tcp …	关闭系统收发 TCP 包的相关的 debugging 开关。	特权模式
debug ospf …	打开 OSPF 协议诊断的相关的 debugging 开关。	特权模式
no debug ospf …	关闭 OSPF 协议诊断的相关的 debugging 开关。	特权模式
debug rip …	打开 RIP 协议诊断的相关的 debugging 开关。	特权模式
no debug rip …	关闭 RIP 协议诊断的相关的 debugging 开关。	特权模式
debug vrrp …	打开 VRRP 协议诊断的相关的 debugging 开关。	特权模式
no debug vrrp …	关闭 VRRP 协议诊断的相关的 debugging 开关。	特权模式
debug mstp …	打开 MSTP 协议诊断的相关的 debugging 开关。	特权模式
no debug mstp …	关闭 MSTP 协议诊断的相关的 debugging 开关。	特权模式
debug igmp	打开 IGMP SNOOPING 功能	特权模式

snooping …	诊断的相关的 debugging 开关。	
no debug igmp snooping …	关闭IGMP SNOOPING功能诊断的相关的 debugging 开关。	特权模式
debug dhcp-relay …	打开 DHCP REALY 协议诊断的相关的 debugging 开关。	特权模式
no debug dhcp-relay …	关闭 DHCP RELAY 协议诊断的相关的 debugging 开关。	特权模式
debug igmp …	打开 IGMP 协议诊断的相关的 debugging 开关。	特权模式
no debug igmp …	关闭 IGMP 协议诊断的相关的 debugging 开关。	特权模式
debug pim sparse-mode …	打开 PIM-SM 协议诊断的相关的 debugging 开关。	特权模式
no debug pim sparse-mode …	关闭 PIM-SM 协议诊断的相关的 debugging 开关。	特权模式
no debug all	关闭系统所有的 debugging 开关。	特权模式

21.2.4 查看 debugging 信息

查看 debugging 信息的命令如下：

命令	描述	CLI 模式
show debugging [ip | ospf | rip | vrrp | mstp | igmp snooping | dhcp-relay | igmp | pim sparse-mode]	查看 debugging 开关配置。如果没有输入参数，查看所有模块的 debugging 开关配置，如果只输入其中一个参数，则只查看一个模块的 debugging 开关配置。如果输入的参数是 ip，则会查看 IP，ICMP， ARP， UDP， TCP 模块的 debugging 开关配置。	普通模式，特权模式